PayPal™

Payflow Pro Fraud Protection Services User's Guide

For Professional Use Only
Currently only available in English.

A usage Professional Uniquement
Disponible en Anglais uniquement pour l'instant.

Last updated: June 2008

Payflow Pro Fraud Protection Services User's Guide

Document Number: 200011.en_US-200806

© 2008 PayPal, Inc. All rights reserved. PayPal is a registered trademark of PayPal, Inc. The PayPal logo is a trademark of PayPal, Inc. Other trademarks and brands are the property of their respective owners.
The information in this document belongs to PayPal, Inc. It may not be used, reproduced or disclosed without the written approval of PayPal, Inc.
Copyright © PayPal. All rights reserved. PayPal S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Registered office: 22-24 Boulevard Royal, L-2449, Luxembourg, R.C.S. Luxembourg B 118 349
Consumer advisory: The PayPal™ payment service is regarded as a stored value facility under Singapore law. As such, it does not require the approval of the Monetary Authority of Singapore. You are advised to read the terms and conditions carefully.

Notice of non-liability:
PayPal, Inc. is providing the information in this document to you "AS-IS" with all faults. PayPal, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. PayPal, Inc. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. PayPal, Inc. reserves the right to make changes to any information herein without further notice.

Content

Preface 9

Intended Audience 9
Document Conventions 9
Document Organization 9
Customer Service 10
Revision History 10

Chapter 1 Overview. 11

Growing Problem of Fraud 11
Reducing the Cost of Fraud 11

Chapter 2 How Fraud Protection Services Protect You 13

The Threats 13
Hacking 13
Credit Card Fraud 13
Protection Against the Threats—Fraud Filters 13
Example Filter 14
Configuring the Filters 14
Reviewing Suspicious Transactions 14
Special Considerations. 14
Merchants With an Instant Fulfillment Model 14
Merchants using the Recurring Billing Service 14

Chapter 3 Configuring the Fraud Protection Services Filters 15

Phase 1: Run Test Transactions Against Filter Settings on Test Transaction Security Servers . 16
Phase 2: Run Live Transactions on Live Transaction Servers in Observe Mode 17
Phase 3: Run All Transactions Through the Live Transaction Security Servers Using Active Mode 18

Chapter 4 Assessing Transactions that Triggered Filters 19

Reviewing Suspicious Transactions 19

Acting on Transactions that Triggered Filters . . . 22
Rejecting Transactions . . . 22
Fine-tuning Filter Settings—Using the Filter Scorecard . . . 22
Ensuring Meaningful Data on the Filter Scorecard . . . 23
Re-running Transactions That Were Not Screened . . . 24

Chapter 5 Activating and Configuring the Buyer Authentication Service 25

Building Customer Confidence . . . 25
Enrolling for the Buyer Authentication Service . . . 25
Downloading the Payflow (Including APIs and API Documentation) . . . 25
Configuring Buyer Authentication . . . 26
Generate Transaction Request Software . . . 27
Testing and Activating the Service . . . 28

Chapter 6 Performing Buyer Authentication Transactions Using the SDK31

Testing the Buyer Authentication Service . . . 31
Buyer Authentication Transaction Overview . . . 31
Buyer Authentication Terminology . . . 32
Buyer Authentication Server URLs . . . 33
Detailed Buyer Authentication Transaction Flow . . . 33
Call 1: Verify that the cardholder is enrolled in the 3-D Secure program . . . 33
Call 2: POST the authentication request to and redirect the customer's browser to the ACS URL . . . 34
Call 3: Validate the PARES authentication data returned by the ACS server . . . 36
Call 4: Submit the intended transaction request to the Payflow server . . . 36
Example Buyer Authentication Transactions . . . 37
Example Verify Enrollment Transaction . . . 38
Example Verify Enrollment Response . . . 38
Example Validate Authentication Transaction . . . 38
Example Payflow Authorization or Sale Transaction . . . 39
Buyer Authentication Transaction Parameters and Return Values . . . 40
Transaction Parameters . . . 40
Verify Enrollment Transaction Name-Value Pairs . . . 40
Validate Authentication Transaction Name-Value Pairs . . . 42
Standard Payflow Sale or Authorization Transaction . . . 43
ECI Values . . . 45

Logging Transaction Information 47
Audit Trail and Transaction Logging 47

Chapter 7 Screening Transactions Using the Payflow SDK 49

Downloading the Payflow SDK (Including APIs and API Documentation) 49
Transaction Data Required by Filters 49
Transaction Parameters Unique to the Filters 52
Existing Payflow Parameters Used by the Filters 53
Response Strings for Transactions that Trigger Filters 54
RESULT Values Specific to Fraud Protection Services 57
Changing the Verbosity Setting 58
Example Response for an Authentication Transaction With Verbosity=Low 58
Example Response for an Authentication Transaction With Verbosity=Medium 58
Accepting or Rejecting Transactions That Trigger Filters 62
Logging Transaction Information 62

Chapter 8 Responses to Credit Card Transaction Requests 65

An Example Response String 65
Contents of a Response to a Credit Card Transaction Request 66
PNREF Value 67
PNREF Format 67
RESULT Codes and RESPMSG Values 68
RESULT Values for Transaction Declines or Errors 68
RESULT Values for Communications Errors 73

Appendix A Fraud Filter Reference 77

Filters Included with the Fraud Protection Services 77
Filters Included with the Basic Fraud Protection Services Option 77
Filters Included with the Advanced Fraud Protection Services Option 78
Special Case: Buyer Authentication Failure Filter 78
About the Fraud Risk Lists 78
Filters Applied After Processing 79
Transaction Data Required by Filters 79
Unusual Order Filters 79
Total Purchase Price Ceiling Filter 79
Total Item Ceiling Filter 80
Shipping/Billing Mismatch Filter 80

Product Watch List Filter . . . 81
High-risk Payment Filters . . . 81
AVS Failure Filter . . . 81
Card Security Code Failure Filter . . . 83
Buyer Authentication Failure Filter . . . 84
BIN Risk List Match Filter . . . 86
Account Number Velocity Filter . . . 86
High-risk Address Filters . . . 86
ZIP Risk List Match Filter . . . 87
Freight Forwarder Risk List Match Filter . . . 87
USPS Address Validation Failure Filter . . . 87
IP Address Match Filter . . . 88
Email Service Provider Risk List Match Filter . . . 88
Geo-location Failure Filter . . . 89
IP Address Velocity Filter . . . 90
High-risk Customer Filters . . . 90
Bad Lists . . . 90
International Order Filters . . . 91
Country Risk List Match Filter . . . 91
International Shipping/Billing Address Filter . . . 91
International IP Address Filter . . . 92
International AVS Filter . . . 92
Accept Filters . . . 93
Good Lists . . . 93
Total Purchase Price Floor Filter . . . 94
Custom Filters . . . 94

Appendix B Testing the Transaction Security Filters . . . 95

Good and Bad Lists . . . 95
AVS Failure Filter . . . 96
BIN Risk List Match Filter . . . 96
Country Risk List Match Filter . . . 97
Email Service Provider Risk List Match Filter . . . 98
Freight Forwarder Risk List Match Filter . . . 98
Geo-location Failure Filter . . . 99
International AVS Filter . . . 99
International IP Address Filter . . . 100
International Shipping/Billing Address Filter . . . 101

IP Address Match Filter 102
Shipping/Billing Mismatch Filter 102
Total Item Ceiling Filter 103
Total Purchase Price Ceiling Filter 103
Total Purchase Price Floor Filter 104
USPS Address Validation Failure Filter 104
ZIP Risk List Match Filter 105

Appendix C Testing Buyer Authentication Transactions Using the Payflow SDK 107

Testing Buyer Authentication Transactions 107
Buyer Authentication Test Server 107
Payflow Test Server 107
Test Case Descriptions and Account Numbers 107
Test Cases 108
Expected Result Codes for Buyer Authentication 109
Buyer Authentication Testing Procedures 110
Perform the Verify Enrollment Transaction 110
Verify Enrollment Transaction Test Cases 111
Example Return Values 111
Validate Authentication Transaction Test Cases 113
Procedure 113
Example Return Values 115

Appendix D Deactivating Fraud Protection Services 117

Index 119

Preface

This document describes Fraud Protection Services and explains how you can use the Payflow SDK to perform transactions that will be screened by Fraud Protection Services filters.

For details on how to configure and use Fraud Protection Services and to generate Buyer Authentication reports through PayPal Manager, see PayPal Manager online help.

Intended Audience

This document is intended for Payflow Pro merchants who subscribe to any Fraud Protection Services options.

Document Conventions

This document uses the term *fraudster* to represent an entity (typically a person) attempting fraudulent activity.

Document Organization

- Chapter 1, "Overview," presents the Fraud Protection Services suite.
- Chapter 2, "How Fraud Protection Services Protect You," describes the security tools that make up the Fraud Protection Services.
- Chapter 3, "Configuring the Fraud Protection Services Filters," describes how to configure Fraud Protection Services.
- Chapter 4, "Assessing Transactions that Triggered Filters," makes recommendations on how to set up and fine-tune filters.
- Chapter 5, "Activating and Configuring the Buyer Authentication Service," describes activating and configuring the Buyer Authentication service.
- Chapter 6, "Performing Buyer Authentication Transactions Using the SDK," describes and provides an example of how to use Buyer Authentication.
- Chapter 7, "Screening Transactions Using the Payflow SDK,"describes how to screen transactions for fraud using the Payflow SDK.
- Chapter 8, "Responses to Credit Card Transaction Requests," describes the responses to a credit card transaction request.

- Appendix A, "Fraud Filter Reference," describes the Transaction filters that make up part of the Fraud Protection Services.
- Appendix B, "Testing the Transaction Security Filters," provides Payflow SDK transactions that you can use to test the filters.
- Appendix C, "Testing Buyer Authentication Transactions Using the Payflow SDK, provides examples of testing Buyer Authentication transactions.
- Appendix D, "Deactivating Fraud Protection Services," describes the process of deactivating Fraud Protection Services.

Customer Service

If you are having problems with Fraud Protection Services, contact Customer Service at:

Email: payflow-support@paypal.com.

Telephone: 1 800 505-4916

Revision History

TABLE 2.1 Revision History

Date	Description
June 2008	Updated Payflow server test and live URLs. Updated Customer Service information.
February 2008	Updated test and live URLs. Minor edits for technical accuracy.
August 2007	AU Enhancements
April 2007	Updated guide to include PayPal Manager User Interface changes.
February 2007	Updated AVS responses rules. Added return codes: 51, 110, 119, 120, 121, 132, 133, 200, 201, 402, 403, 404, 600, and 601.
December 2006	Updated buyer auth test URL to pilot-buyerauth.verisign.com Minor corrections for technical accuracy

1 Overview

This chapter discusses how fraud can affect you the merchant and provides an overview of Fraud Protection Services.

In This Chapter

- "Growing Problem of Fraud" on page 11
- "Reducing the Cost of Fraud" on page 11

Growing Problem of Fraud

Online fraud is a serious and growing problem. While liability for fraudulent card-present or in-store transactions lies with the credit card issuer, liability for card-not-present transactions, including transactions conducted online, *falls to the merchant*. As you probably know, this means that a merchant that accepts a fraudulent online transaction (even if the transaction is approved by the issuer) does not receive payment for the transaction and additionally must often pay penalty fees and higher transaction rates. (One notable exception, Buyer Authentication, is described in this document.)

Reducing the Cost of Fraud

Fraud Protection Services, in conjunction with your Payflow Pro service's standard security tools, can help you to significantly reduce these costs and the resulting damage to your business.

NOTE: Merchants must meet the following eligibility requirements to enroll in and use the Fraud Protection Services products:

- Merchant must have a current, paid-in-full Payflow Pro service account.
- Merchant Payflow Pro service account must be activated (in Live mode).
- Merchant must have its business operations physically based in the United States of America.
- Merchant must use one of the following terminal-based processors: American Express Phoenix, FDMS Nashville, FDMS North, FDMS South, Global Payments East, Nova, Paymentech New Hampshire, or Vital.

2 How Fraud Protection Services Protect You

This chapter describes the security tools that make up the Fraud Protection Services.

In This Chapter

- "The Threats" on page 13
- "Protection Against the Threats—Fraud Filters" on page 13
- "Special Considerations" on page 14

The Threats

There are two major types of fraud—hacking and credit card fraud.

Hacking

Fraudsters *hack* when they illegally access your customer database to steal card information or to take over your Payflow Pro account to run unauthorized transactions (purchases and credits). Fraud Protection software *filters* minimize the risk of hacking by enabling you to place powerful constraints on access to and use of your PayPal Manager and Payflow Pro accounts.

Credit Card Fraud

Fraudsters can use stolen or false credit card information to perform purchases at your Web site, masking their identity to make recovery of your goods or services impossible. To protect you against credit card fraud, the Fraud Protection filters identify potentially fraudulent activity and let you decide whether to accept or reject the suspicious transactions.

Protection Against the Threats—Fraud Filters

Configurable filters screen each transaction for evidence of potentially fraudulent activity. When a filter identifies a suspicious transaction, the transaction is marked for review.

Fraud Protection Services offers two levels of filters: Basic and Advanced. The filters are described in Appendix B, "Fraud Filter Reference."

For detailed descriptions of the filter levels, the order and logic of the screening process, and for specific variations from the simple flow described here, see Appendix A, "How Filters Work."

Example Filter

The Total Purchase Price Ceiling filter compares the total amount of the transaction to a maximum purchase amount (the ceiling) that you specify. Any transaction amount that exceeds the specified ceiling triggers the filter.

Configuring the Filters

Through PayPal Manager, you configure each filter by specifying the action to take whenever the filter identifies a suspicious transaction (either set the transaction aside for review or reject it). See PayPal Manager online help for detailed filter configuration procedures.

Typically, you specify setting the transaction aside for review. For transactions that you deem extremely risky (for example, a known bad email address), you might specify rejecting the transaction outright. You can turn off any filter so that it does not screen transactions.

For some filters, you also set the value that triggers the filter—for example the dollar amount of the ceiling price in the Total Purchase Price Ceiling filter.

Reviewing Suspicious Transactions

As part of the task of minimizing the risk of fraud, you review each transaction that triggered a filter through PayPal Manager to determine whether to accept or reject the transaction. See PayPal Manager online help for details.

Special Considerations

Merchants With an Instant Fulfillment Model

For businesses with instant fulfillment business models (for example, software or digital goods businesses), the **Review** option does not apply to your business—you do not have a period of delay to review transactions before fulfillment to customers. Only the **Reject** and **Accept** options are applicable to your business model.

In the event of server outage, Fraud Protection Services is designed to queue transactions for online processing. This feature also complicates an instant fulfillment business model.

Merchants using the Recurring Billing Service

To avoid charging you to filter recurring transactions that you know are reliable, Fraud Protection Services filters do not screen recurring transactions.

To screen a prospective recurring billing customer, submit the transaction data using PayPal Manager's Virtual Terminal. The filters screen the transaction in the normal manner. If the transaction triggers a filter, then you can follow the normal process to review the filter results.

3 Configuring the Fraud Protection Services Filters

This chapter describes how to configure the Fraud Filters for your Payflow Pro account. The chapter explains a phased approach to implementing the security of transactions. You are not required to use the approach described in this chapter. However it enables you to fine tune your use of filters before you actually deploy them in a live environment.

You first make and fine-tune filter settings in a test environment. Then you move to a live transaction environment to fine-tune operation in an **Observe**-only mode. Finally, when you are fully satisfied with your settings, you move to live **Active** mode to begin screening all live transactions for fraud.

Filter operation is fully described in Appendix A, "Fraud Filter Reference."

IMPORTANT: *Upon completing the configuration procedures within each of the phases described below, you must click the **Deploy** button to deploy the filter settings. Filter settings take effect only after you deploy them.*

Filter setting changes are updated hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect. This waiting period only occurs when you move from one mode to the next.

- **Phase 1:** Run test transactions in **Test** mode using test transaction servers

  In the test phase of implementation, you configure fraud filter settings for test servers that do not affect the normal flow of transactions. You then run test transactions against the filters and review the results offline to determine whether the integration was successful. Once you are happy with the filter settings, you move to the next phase and the settings that you decided upon in the test phase are transferred to the live servers.

- **Phase 2:** Run live transactions on live transaction security servers using **Observe** mode

  When you deploy to Observe mode, the settings that you decided upon in the test phase are automatically transferred to the live servers.

  In Observe mode, the filters examine each live transaction and mark the transaction with each triggered filter's action. You can then view the actions that would have been taken on the live transactions had the filters been active. Regardless of the filter actions, all transactions are submitted for processing in the normal fashion.

- **Phase 3:** Run live transactions on live transaction security servers using **Active** mode

  Once you have set all filters to the optimum settings, you deploy the filters to Active mode. In Active mode, filters on the live servers examine each live transaction and take the specified action when triggered.

  NOTE: Remember that you can test a new filter setting using the test servers at any time (even if your account is in Active mode), and then, if desired, make an adjustment to the live filter settings.

Phase 1: Run Test Transactions Against Filter Settings on Test Transaction Security Servers

In this phase of implementation, you configure filter settings for test servers that do not affect the normal flow of live transactions. You then run test transactions against the filters and review the results offline to determine whether the integration was successful. Continue modifying and testing filters as required.

NOTE: There is no per-transaction fee when you use the test servers.

1. In the Service Summary section of the PayPal Manager home page, click the Basic or Advanced Fraud Protection link.

   Click **Service Settings > Fraud Protection >Test Setup**.

2. Click **Edit Standard Filters**. The *Edit Standard Filters* page appears.

3. For each filter:

   – Click the filter check box to enable it and click-to-clear the check box to disable it.
   – Select the filter action that should take place when the filter is triggered.

   For some filters, you set a trigger value. For example, the Total Purchase Price Ceiling filter trigger value is the transaction amount that causes the filter to set a transaction aside.

   NOTE: To make decisions about how the filters work, see Appendix B, "Fraud Filter Reference."

   NOTE: If you have not enrolled for the Buyer Authentication Service, then the Buyer Authentication Failure filter is grayed-out and you cannot configure it.

   Items that you enter in the Test **Good**, **Bad**, or **Product Watch** lists are not carried over to your configuration for the live servers, so do not spend time entering a complete list for the test configuration. For details on the **Good**, **Bad**, or **Product Watch** list filters, see Appendix B, "Fraud Filter Reference."

4. Once you complete editing the page, click **Deploy**.

   IMPORTANT: *If you do not deploy the filters, then your settings are not saved.*

5. All filters are now configured, and you can begin testing the settings by running test transactions. Follow the guidelines outlined in Appendix B, "Testing the Transaction Security Filters." To run test transactions, you can use PayPal Manager's Virtual Terminal. See PayPal Manager for online help instructions.

6. Review the filter results by following the instructions in Chapter 4, "Assessing Transactions that Triggered Filters."

7. Based on your results, you may want to make changes to the filter settings. Simply return to the Edit Filters page, change settings, and redeploy them. Once you are happy with your filter settings, you can move to Phase 2.

Phase 2: Run Live Transactions on Live Transaction Servers in Observe Mode

In this phase, you configure filters on live servers to the settings that you had fine-tuned on the test servers. In Observe mode, filters examine each live transaction and mark the transaction with the filter results. The important difference between Observe and Active mode is that, regardless of the filter actions, all Observe mode transactions are submitted for processing in the normal fashion.

Observe mode enables you to view filter actions offline to assess their impact (given current settings) on your actual transaction stream.

NOTE: You are charged the per-transaction fee to use the live servers in either Observe or Active mode.

1. Click **Service Settings > Fraud Protection >Test Setup**. Click **Move Test Filter Settings to Live**. The **Move Test Filter Setting to Live** page appears. Remember that in this phase, you are configuring the live servers.
2. Click **Move Test Filter Settings to Live**. On the page that appears, click **Move Test Filter Settings to Live** again.
3. The *Move Test Filter Settings to Live* page prompts whether to deploy the filters in **Observe** modeor in **Active** mode. Click **Deploy to Observe Mode**.

Once you deploy the filters, all transactions are sent to the live servers for screening by the live filters. In **Observe** mode, each transaction is marked with the filter action that would have occurred (Review, Reject, or Accept) had you set the filters to **Active** mode

This enables you to monitor (without disturbing the flow of transactions) how actual customer transactions would have been affected by active filters.

IMPORTANT: *Deployed filter setting changes are updated hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect. This waiting period only occurs when you move from one mode to the next.*

4. Perform testing of the filters. Follow the procedures outlined in Appendix B, "Testing the Transaction Security Filters."
5. Review the filter results by following the instructions in Chapter 4, "Assessing Transactions that Triggered Filters." The Filter Scorecard (described on page 22) will be particularly helpful in isolating filter performance that you should monitor closely and in ensuring that a filter setting is not set so strictly so as to disrupt normal business.
6. Once you are happy with your filter settings, you can move to Phase 3.

Phase 3: Run All Transactions Through the Live Transaction Security Servers Using Active Mode

Once you have configured all filters to optimum settings, you convert to **Active** mode. Filters on the live servers examine each live transaction and take the specified action.

7. Click **Move Test Filter Settings to Live**. On the page that appears, click **Move Test Filter Settings to Live** again.
8. On the *Move Test Filter Settings to Live* page, click **Deploy to Active Mode**.

   At the top of the next hour, all live transactions will be inspected by the filters.
9. Use the instructions in Chapter 4, "Assessing Transactions that Triggered Filters," to detect and fight fraud.

IMPORTANT: *Remember that you can make changes to fine-tune filter settings at any time. After changing a setting, you must re-deploy the filters so that the changes take effect.*

4 Assessing Transactions that Triggered Filters

As part of the task of minimizing the risk of fraud, you review each transaction that triggered a filter. You decide, based on the transaction's risk profile, whether to accept or reject the transaction. This chapter describes how to review transactions that triggered filters, and provides guidance on deciding on risk.

NOTE: The Fraud Protection Services package (Basic or Advanced) to which you subscribe determines the number of filters that screen your transactions. Basic subscribers have access to a subset of the filters discussed in this chapter. Advanced subscribers have full access. See "Filters Included with the Fraud Protection Services" on page 83 for complete lists of Basic and Advanced filters.

In This Chapter

- "Reviewing Suspicious Transactions" on page 19
- "Fine-tuning Filter Settings—Using the Filter Scorecard" on page 22
- "Re-running Transactions That Were Not Screened" on page 24

Reviewing Suspicious Transactions

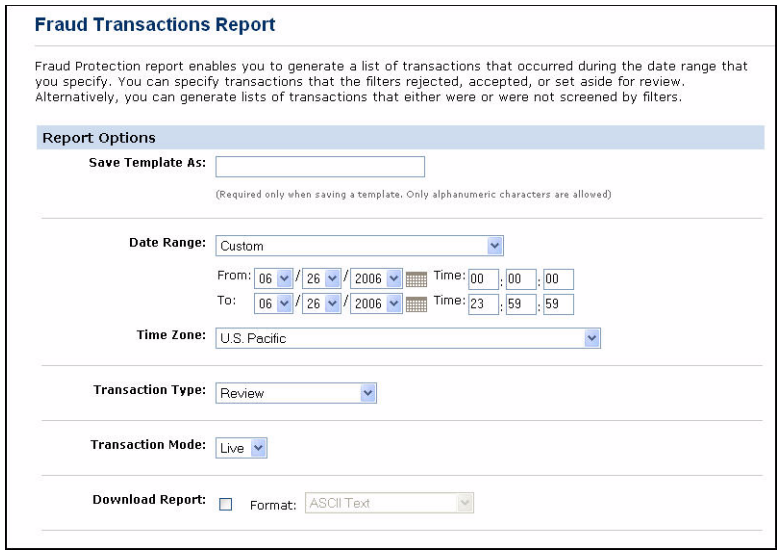
Transactions that trigger filters might or might not represent attempted fraud. It is your responsibility to analyze the transaction data and then to decide whether to accept or reject the transaction. Accepting a transaction requires no further action. To reject a transaction, a separate void of the transaction is required.

The first step in reviewing filtered transactions is to list the transactions.

1. Click **Reports > Fraud Protection > Fraud Transactions**

   The *Fraud Transactions Report* page appears.

FIGURE 4.1 Fraud Transactions Report page


Fraud Transactions Report
Fraud Protection report enables you to generate a list of transactions that occurred during the date range that you specify. You can specify transactions that the filters rejected, accepted, or set aside for review. Alternatively, you can generate lists of transactions that either were or were not screened by filters.
Report Options
Save Template As:
(Required only when saving a template. Only alphanumeric characters are allowed)
Date Range:
Custom
From: 06 / 26 / 2006 Time: 00 : 00 : 00
To: 06 / 26 / 2006 Time: 23 : 59 : 59
Time Zone:
U.S. Pacific
Transaction Type:
Review
Transaction Mode:
Live
Download Report:
Format:
ASCII Text

2. Specify the date range of the transactions to review.
3. Specify a **Transaction Type**:

TABLE 4.1 Transaction types

Transaction Type	Description
Reject	Transactions that the filters rejected. These transactions cannot be settled. The type of filter that took this action is called a *Reject filter*.
Review	Transactions that the filters set aside for your review. The type of filter that took this action is called a *Review filter*.
Accept	Transactions that the filters allowed through the normal transaction submission process. The type of filter that took this action is called an *Accept filter*.
Not Screened by Filters	Transactions that were not screened by any filter. This condition (Result Code 127) indicates that an internal server error prevented the filters from examining transactions. This conditional occurs only in Test mode or Live mode. In Observe mode all results codes are always 0. You can re-screen any of these transactions through the filters as described in "Re-running Transactions That Were Not Screened" on page 24.
Screened by Filters	All transactions that were screened by filters, regardless of filter action or whether any filter was triggered.

4. Specify the Transaction Mode, and click **Run Report**.

   The *Fraud Transactions Report* page displays all transactions that meet your search criteria.

NOTE: If filters are deployed in Observe mode, then all transactions have been submitted for processing and are ready to settle. Transactions are marked with the action that the filter would have taken had the filters been deployed in Active mode.

The following information appears in the report:

TABLE 4.2 Transactions Report field descriptions

Heading	Description
Report Type	The type of report created.
Date	Date and time range within which the transactions in this report were run.
Time Zone	Time zone represented in this report.
Transaction Mode	Test, Observe, or Active
Transaction ID	Unique transaction identifier. Click this value to view the *Transaction Detail* page.
Transaction Time	Time and date that the transaction occurred.
Transaction Type	The transaction status that resulted from filter action, as described in Table 4.1.
Card Type	MasterCard or Visa.
Amount	Amount of the transaction.

The following transaction status values can appear in the report:

TABLE 4.3 Transaction status values

Stage of Review	Transaction Status	Result Code	Result Message	Report in Which the Transaction Appears
Screened by filters	Pass	0	Approved	Approved report
Screened by filters	Review	126	Under Review by Fraud Service	Approved report
Screened by filters	Reject	125	Declined by Fraud Service	Declined report
Screened by filters	Accept	0	Approved	Approved report
Screened by filters	Service Outage	127	Unprocessed by Fraud Service	Approved report
After review by merchant	Accepted	0	Approved	Approved report
	Rejected	128	Declined by Merchant	Declined report

Click the **Transaction ID** of the transaction of interest.

The *Fraud Details* page appears, as discussed in the next section.

Acting on Transactions that Triggered Filters

The *Fraud Details* page displays the data submitted for a single transaction. The data is organized to help you to assess the risk types and to take action (accept, reject, or continue in the review state).

The following notes describe data in the Fraud Details page shown in the figure.

1. This transaction was set aside because it triggered the AVS Failure filter.
2. The transaction was not screened by any of the filters in the Skipped Filters section because the data required by these filters did not appear in the transaction data or was badly formatted. In special cases, all filters appear here. See "Re-running Transactions That Were Not Screened" on page 24
3. Specify the action to take on the transaction:
   - Review: Take no action. You can return to this page at any time or reject or accept the transaction. The transaction remains unsettleable.
   - Reject: Do not submit the transaction for processing. See "Rejecting Transactions" on page 22.
   - Accept: Submit the transaction for normal processing.
4. You can enter notes regarding the disposition of the transaction or the reasons for taking a particular action. Do not use the & < > or = characters.
5. Click **Submit** to save the notes, apply the action, and move to the next transaction.

NOTE: You can also view the *Fraud Details* page for transactions that were rejected or accepted. While you cannot change the status of such transactions, the page provides insight into filter performance.

Rejecting Transactions

If you decide to reject a transaction, you should notify the customer that you could not fulfill the order. Do not be explicit in describing the difficulty with the transaction because this provides clues for performing successful fraudulent transactions in the future. Rejected transactions are never settled.

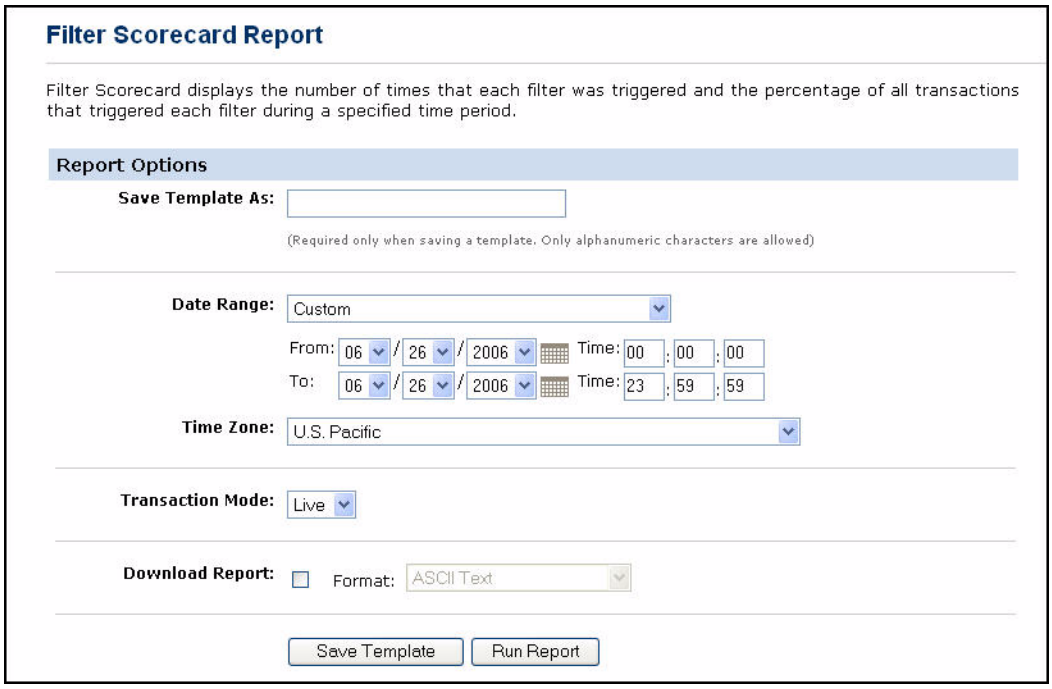
Fine-tuning Filter Settings—Using the Filter Scorecard

The Filter Scorecard displays the number of times that each filter was triggered and the percentage of all transactions that triggered each filter during a specified time period.

This information is especially helpful in fine-tuning your risk assessment workflow. For example, if you find that you are reviewing too many transactions, then use the Filter Scorecard to determine which filters are most active. You can reduce your review burden by relaxing the settings on those filters (for example, by setting a higher amount for the Purchase Price Ceiling filter).

1. Click **Reports > Filter Scorecard**. The *Filter Scorecard Report* page appears.

FIGURE 4.2 Filter Scorecard Report page


Filter Scorecard Report
Filter Scorecard displays the number of times that each filter was triggered and the percentage of all transactions that triggered each filter during a specified time period.
Report Options
Save Template As:
(Required only when saving a template. Only alphanumeric characters are allowed)
Date Range:
Custom
From: 06 / 26 / 2006 Time: 00 : 00 : 00
To: 06 / 26 / 2006 Time: 23 : 59 : 59
Time Zone:
U.S. Pacific
Transaction Mode:
Live
Download Report:
Format:
ASCII Text
Save Template
Run Report

2. Specify the date range of the transactions to review.
3. In the **Transaction Mode** field, specify transactions screened by the live or the test servers.
4. Click **Run Report**.

   The *Filter Scorecard Report* page displays the number of times that each filter was triggered and the percentage of all transactions that triggered each filter during the time span that you specified.

Ensuring Meaningful Data on the Filter Scorecard

The Scorecard shows the total number of triggered transactions for the time period that you specify, so if you had changed a filter setting during that period, the Scorecard result for the filter might reflect transactions that triggered the filter at several different settings.

Say, for example, you changed the Total Purchase Price Ceiling on August 1 and again on August 7. You then run a Filter Scorecard for July 1 to August 31. Between July 1 to August

31, three different price ceiling settings caused the filter to trigger, yet the Scorecard would not indicate this fact.

To ensure meaningful results in the Filter Scorecard, specify a time period during which the filter settings did not change.

Re-running Transactions That Were Not Screened

Perform the following steps if you wish to re-run a transaction that was not screened by filters (transactions with Result Code 127):

1. Navigate to **Reports > Fraud Protection > Fraud Transaction Report**. The *Fraud Transaction Report* page appears.
2. Select the appropriate time period for the search, and select the "Not Screened by Filters" option for **Transaction Type**.
3. Click **RunView Report**. The *Fraud Transaction Report Results* page appears. It contains all the transactions that were not screened by filters.
4. Click on the Transaction ID of the transaction you would like to re-run. The *Confirm Rerun* page appears.
5. Click **Yes** to re-run that transaction. The *Success* page appears if your transaction was successful.

NOTE: If multiple attempts at screening fail, then the transaction may have data formatting problems. Validate the data, and contact Customer Service.

If you encounter 50 or more transactions with Result Code 127, then contact Customer Service, who can resubmit them as a group.

5 Activating and Configuring the Buyer Authentication Service

This chapter describes how to enroll, configure, test, and activate the Buyer Authentication Service.

In This Chapter

- "Building Customer Confidence" on page 25
- "Enrolling for the Buyer Authentication Service" on page 25
- "Downloading the Payflow (Including APIs and API Documentation)" on page 25
- "Configuring Buyer Authentication" on page 26
- "Testing and Activating the Service" on page 28

Building Customer Confidence

Buyer Authentication reduces your risk and builds your customers' confidence. The card brands make marketing resources available to you to promote your Web site and logos you can build into your checkout process.

For more information, visit:

- http://usa.visa.com/business/accepting_visa/ops_risk_management/vbv_marketing_support.html

or

- http://www.securecodemerchant.com

Enrolling for the Buyer Authentication Service

To enroll for the Buyer Authentication Service, click the Buyer Authentication banner on the PayPal Manager main page. Follow the on-screen instructions to determine whether both your processor and your acquiring bank support the Buyer Authentication service. If they both support the service, then you can follow the on-screen instructions to enroll.

Downloading the Payflow (Including APIs and API Documentation)

The Payflow software development kit (SDK) is available from the PayPal Manager Downloads page as a .NET or Java library, or you can build your own API by posting directly to the Payflow servers via HTTPS.

IMPORTANT: *Full API documentation is included with each SDK.*

Configuring Buyer Authentication

To enable Buyer Authentication processing on your site, you will need to construct two transaction requests (messages) and construct a frameset. You can accomplish the tasks in a few hours.

In the standard Payflow Pro implementation, when the customer submits a purchase request, your website sends a single Sale transaction request with all purchase details (message with transaction type S) to the server. With Buyer Authentication, you must submit two additional transaction requests (types E— Verify Enrollment and Z—validate PARES response) before the Sale.

Follow these steps:

1. Log in to PayPal Manager at https://paypal.manager.com.
2. Click **Service Settings > Fraud Protection > Buyer Authentication**. The *Buyer Authentication Setup* page appears.
3. Enter Registration information (complete all fields for both MasterCard and Visa).
   - Select your Acquirer (Acquirer Support) for MasterCard and Visa and click Activate to activate the Acquirer you selected.
   - Enter your Business Name.
   - Enter the fully qualified URL (be sure to include http:// or https://) of your business.
   - Select your Country Code from the drop-down menu.
4. Click **Submit**. A gray notification box appears towards the top of the page confirming the changes. If there are any errors, a yellow box appears towards the top of the page stating the problem.
5. On the main PayPal Manager page click the **Download** link.
6. Read chapters 5 through 7 and Appendix D of this document
7. Download the Payflow SDK (Software Developer's Kit) appropriate for your software environment.
8. Download *Payflow Pro Developer's Guide* (PDF format document). Read as much of *Payflow Pro Developer's Guide* as you need.
9. Configure the Payflow SDK as described in the developer's guide.

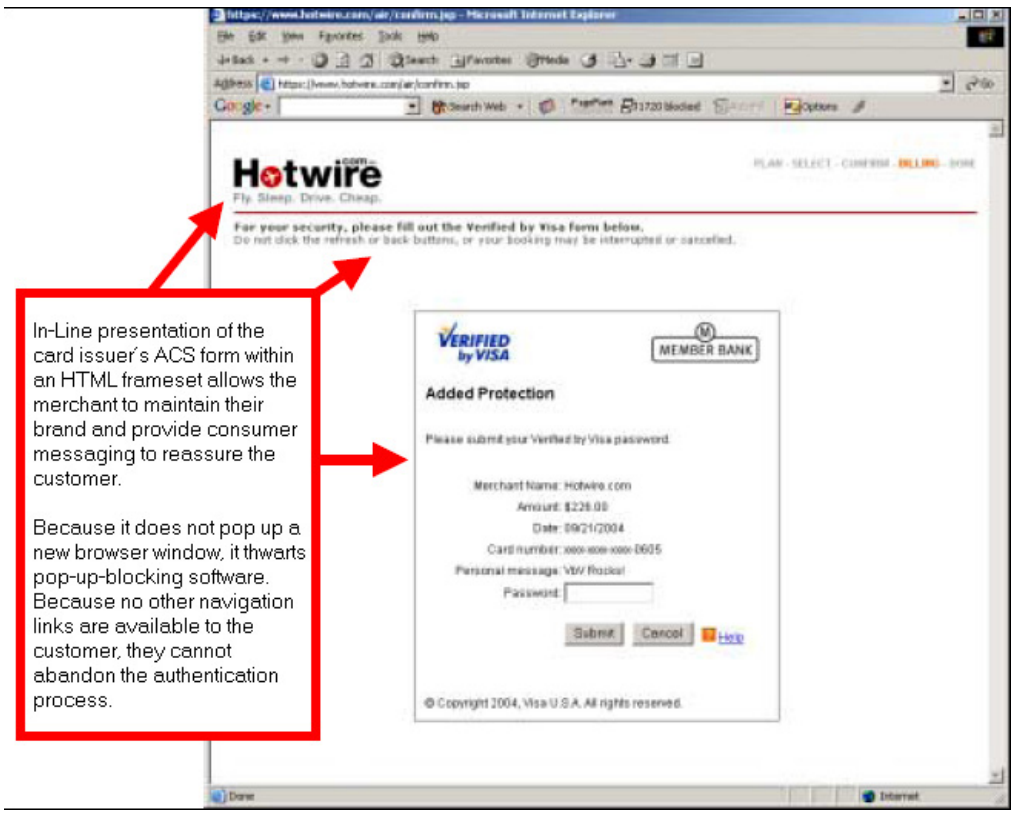
Generate Transaction Request Software

1. Submit a Verify Enrollment transaction request (type E) to determine whether the cardholder is enrolled in either the Verified by Visa or MasterCard SecureCode service. See the example on page 38.
2. The response is either Enrolled or Not Enrolled. See the example responses on page 38.
3. If the customer is enrolled, you populate the response data into a form page (hosted on your server) and post it to the URL of the card issuing bank (ACS) indicated in the response. Make sure the TermUrl field is properly specified, as this is where the ACS will post the response. See "Example ACS Redirect Code" on page 35.
4. The ACS responds to the post by presenting an Authentication window to the customer.

   By Visa/MasterCard requirements, the HTML page for displaying the ACS form must be presented in-line (within the same browser session as the e-commerce transaction), preferably as framed-inline.

   The ACS form should be displayed in a frame set, as shown in the following example. The message across the top of the frame is required.

   NOTE: You should not employ pop-up windows. They will be blocked by pop-up blocking software.


In-Line presentation of the card issuer's ACS form within an HTML frameset allows the merchant to maintain their brand and provide consumer messaging to reassure the customer.
Because it does not pop up a new browser window, it thwarts pop-up-blocking software. Because no other navigation links are available to the customer, they cannot abandon the authentication process.
Hotwire
Fly. Sleep. Drive. Cheap.
For your security, please fill out the Verified by Visa form below.
VERIFIED by VISA
MEMBER BANK
Added Protection
Please submit your Verified by Visa password.
Merchant Name: Hotwire.com
Amount: $226.00
Date: 09/21/2004
Password:
Submit
Cancel
© Copyright 2004, Visa U.S.A. All rights reserved.

5. When the customer enters their password and clicks **Submit**, the ACS verifies the password and posts a response to the TermURL (the page on your site that is configured to receive ACS responses).

6. Submit a Validate Authentication Response transaction request (type Z) to validate (ensure that the message has not been falsified or tampered with) and decompose the Authentication Response from the card-issuing bank (ACS). See "Example Validate Authentication Response" on page 39.

7. The response contains the following data elements:

   – XID
   – Authentication Status
   – ECI. E-commerce Indicator
   – Visa: CAVV. Cardholder Authentication Verification Value

   — or —

   MasterCard: AAV. Accountholder Authentication Value

   Submit these values, along with the standard transaction data, in a standard Sale or Authorization transaction request, as described in "Call 4: Submit the intended transaction request to the Payflow server" on page 36.

Testing and Activating the Service

1. Make these other required UI modifications:

   Payment page pre-messaging. The example text shown below and in the red boxes in the figure must appear on your payment page to advise the customer that authentication may take place.

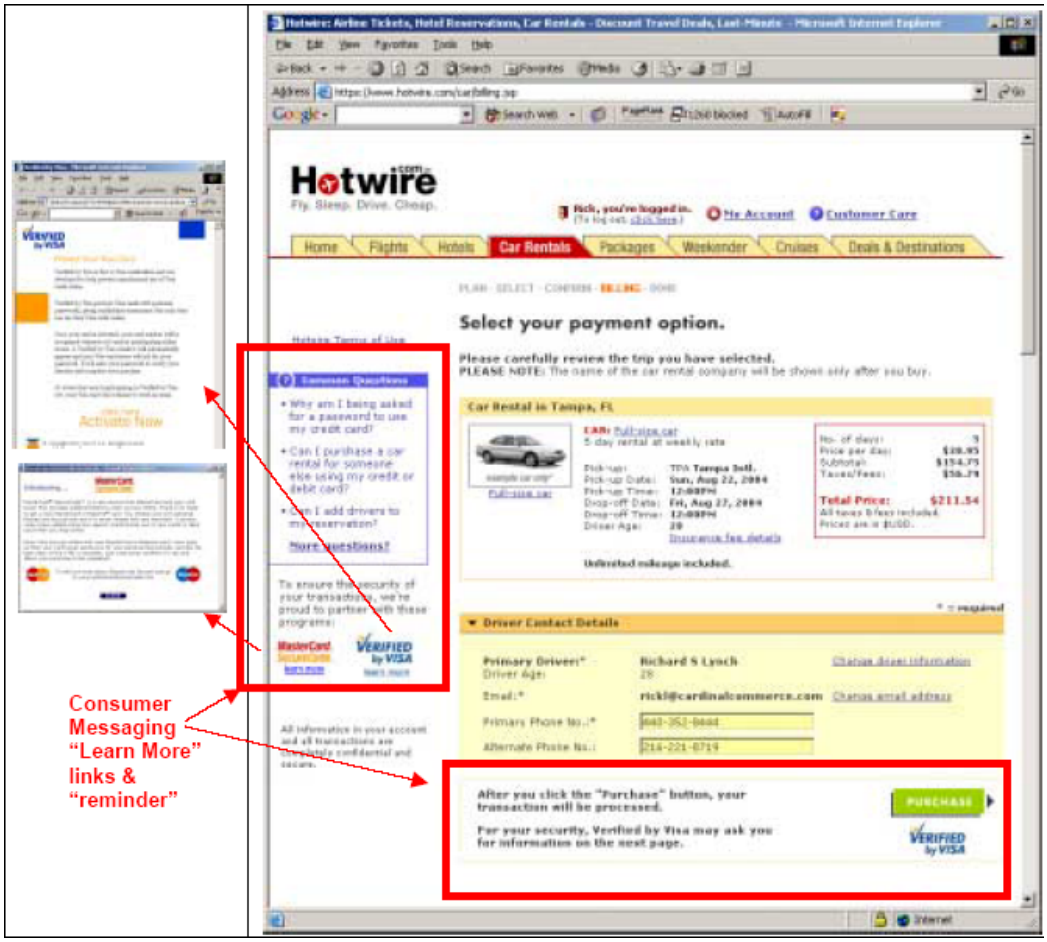
   Example text in "Learn More" box on the left:

- Why am I being asked for a password to use my credit card?
- Can I purchase a car rantal for someone else using my credit or debit card?
- Can I add drivers to my reservation?

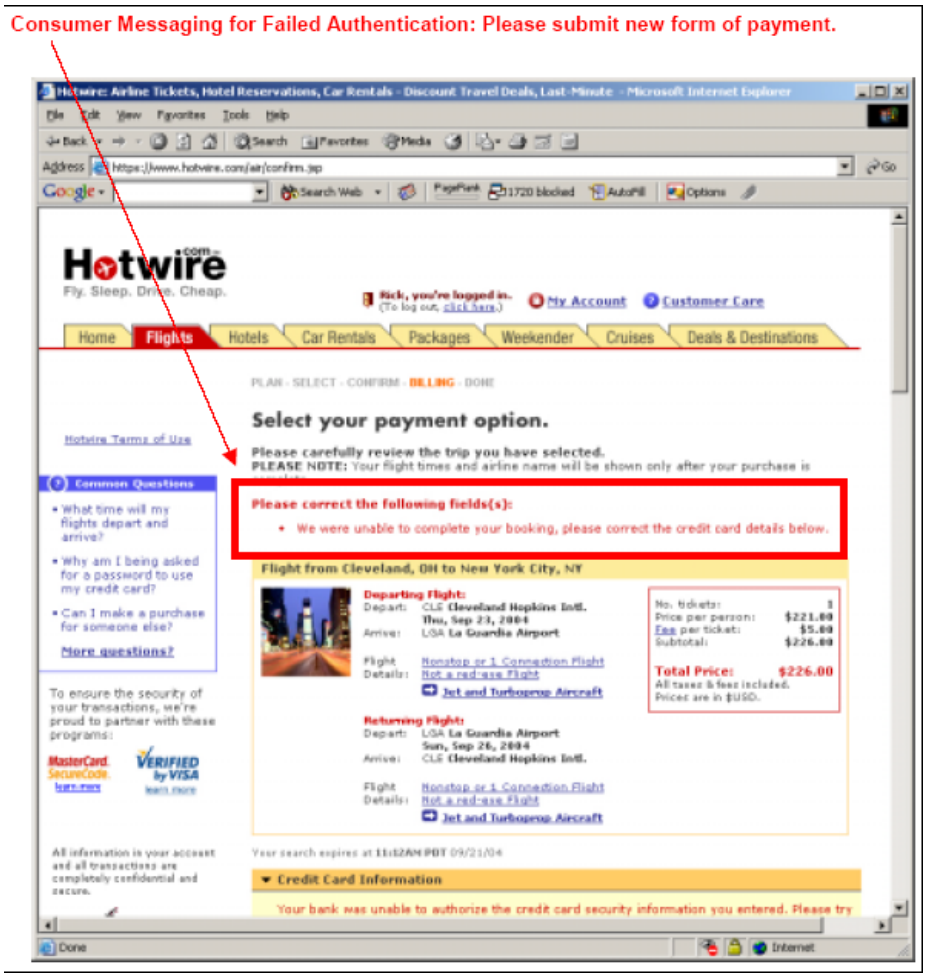
   More questions?

   Example text in "reminder":
   After you check the "Purchase" button, your transaction will be processed.
   For your security, Verified by Visa may ask you for information on the next page.

NOTE: Buyer Authentication can only be activated when Fraud Protection Services is live.



Failure messaging. The example text in the red box handles cases where customers cannot successfully authenticate themselves. The text requests another form of payment.


Consumer Messaging for Failed Authentication: Please submit new form of payment.
Hotwire: Airline Tickets, Hotel Reservations, Car Rentals - Discount Travel Deals, Last-Minute - Microsoft Internet Explorer
Hotwire.com
Fly. Sleep. Drive. Cheap.
Rick, you're logged in.
My Account
Customer Care
Home
Flights
Hotels
Car Rentals
Packages
Weekender
Cruises
Deals & Destinations
Select your payment option.
Please carefully review the trip you have selected.
Please correct the following fields(s):
We were unable to complete your booking, please correct the credit card details below.
Flight from Cleveland, OH to New York City, NY
Credit Card Information
Your bank was unable to authorize the credit card security information you entered. Please try

Consumer Messaging for Failed Authentication: Please submit new form of payment.

2. Perform a last round of test transactions as described in Appendix C, "Testing Buyer Authentication Transactions Using the Payflow SDK," to ensure the flow and screen presentation is correct.

3. Once all message flows and customer messaging and required logos are in place, you can activate Buyer Authentication to accept live transactions.

6 Performing Buyer Authentication Transactions Using the SDK

This chapter describes the process of performing Buyer Authentication transactions using the Payflow SDK. For information on using the SDK and on transaction syntax see *Payflow Pro Developer's Guide*.

The content and format of responses to transaction requests are described in "Buyer Authentication Transaction Parameters and Return Values" on page 40. Standard Payflow Pro response values are described in *Payflow Pro Developer's Guide*.

XMLPay client support for Buyer Authentication is described in *Payflow Pro XMLPay Developer's Guide*.

For information on how to view Buyer Authentication reports in PayPal Manager, see PayPal Manager online help.

Testing the Buyer Authentication Service

Information on testing Buyer Authentication Service transactions appears in Appendix C, "Testing Buyer Authentication Transactions Using the Payflow SDK."

In This Chapter

- "Buyer Authentication Transaction Overview" on page 31
- "Buyer Authentication Terminology" on page 32
- "Buyer Authentication Server URLs" on page 33
- "Detailed Buyer Authentication Transaction Flow" on page 33
- "Example Buyer Authentication Transactions" on page 37
- "Buyer Authentication Transaction Parameters and Return Values" on page 40
- "ECI Values" on page 45
- "Logging Transaction Information" on page 47

Buyer Authentication Transaction Overview

To implement Buyer Authentication, you use the Payflow SDK to write software that:

1. Receives the customer's account number and determines whether it is enrolled in the Verified by Visa or MasterCard SecureCode buyer authentication program.
2. If the cardholder is enrolled, then your program redirects the customer to the issuing bank's buyer authentication page. The customer submits their username and password. The

issuing bank authenticates the customer's identity by returning a payer authentication response value to your program.

3. Your program then validates the authentication response.
4. If the authentication data is valid, then your program submits a standard Payflow authorization or sale transaction that includes the buyer authentication data.

NOTE: The Buyer Authentication Service supports only Sale and Authorization transaction types.

Buyer Authentication Terminology

The following terms are used in this chapter:

TABLE 6.1 Buyer Authentication terminology

Term	Definition
MPI	The Merchant Plug-in software component that implements merchant's client functionalities in 3-D Secure protocol. The 3-D Secure server at https://buyerauth.com/DDDSecure/MerchantPlug-In implements MPI's specification as a payment gateway.
PAREQ	The Payer Authentication Request message that you send to the issuing bank's buyer authentication page.
PARES	Payer Authentication Response, digitally signed by the issuing bank.
CAVV	Cardholder Authentication Verification Value. The value generated by card issuing bank to prove that the cardholder has been authenticated with a particular transaction.
XID	Buyer authentication Transaction ID. Used only by Verified by Visa to identify a unique buyer authentication transaction.
ECI	E-Commerce Indicator. The ECI value indicates the level of security supported by the merchant when the cardholder provided the payment card data for an Internet purchase. When returned in a buyer authentication response, it is determined by the issuing bank.
Authentication Status	Key component in the 3-D Secure protocol. A server run by card issuer performing functionalities of enrolling a card for 3-D Secure, verifying card enrollment, and authenticating cardholder and issuing a digitally signed payment authentication response (PARES).

Buyer Authentication Server URLs

IMPORTANT: *URLs listed here are used only for buyer authentication transactions: Verify Enrollment (TRXNTYPE=E) and Validate Authentication (TRXNTYPE=Z).*

- The production Buyer Authentication server URL is buyerauth.verisign.com
- The test Buyer Authentication server URL is pilot-buyerauth.verisign.com

Detailed Buyer Authentication Transaction Flow

A buyer authentication transaction involves the following four program calls. Examples of exact syntax appear in "Example Buyer Authentication Transactions" on page 37.

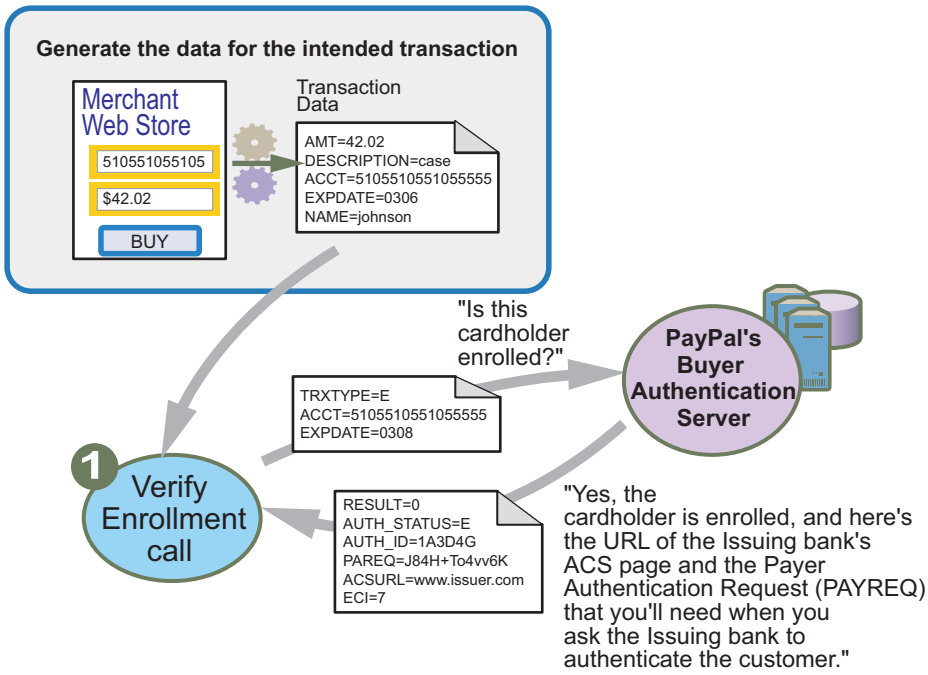
NOTE: XMLPay uses the VerifyEnrollment transaction for Call 1.

Call 1: Verify that the cardholder is enrolled in the 3-D Secure program

For the Verify Enrollment call (VerifyEnrollment transaction in XMLPay), you determine whether the cardholder is enrolled in the 3-D Secure program. Send a transaction (TRXTYPE=E) to the Buyer Authentication server.

The server returns the AUTHENTICATION_STATUS of enrollment (E means enrolled), an AUTHENTICATION_ID value, and an ECI value (electronic commerce indicator, defaulted to 7 [Authentication Unsuccessful] because authentication has not yet occurred). If the cardholder is enrolled, then the message also includes a PAREQ (payer authentication request) value and the ACSURL—the URL of the Issuer's ACS (access control server) page at which buyers provide their password to authenticate themselves. The PAREQ is used in the next call to ask the Issuing bank to authenticate the customer.

If the cardholder is not enrolled (AUTHENTICATION_STATUS=O), cannot be verified (X), or an error occurred (I), skip to Call 4, "Call 4: Submit the intended transaction request to the Payflow server" and submit a standard Payflow authorization or sale transaction that includes the AUTHENTICATION_STATUS, AUTHENTICATION_ID, and ECI values.



Call 2: POST the authentication request to and redirect the customer's browser to the ACS URL

NOTE: XMLPay uses the ValidateAuthentication transaction for Call 2.

If the card is enrolled, you place the following values in an HTTP form and then HTTP POST the values to the ACS URL (the issuer's ACS site):

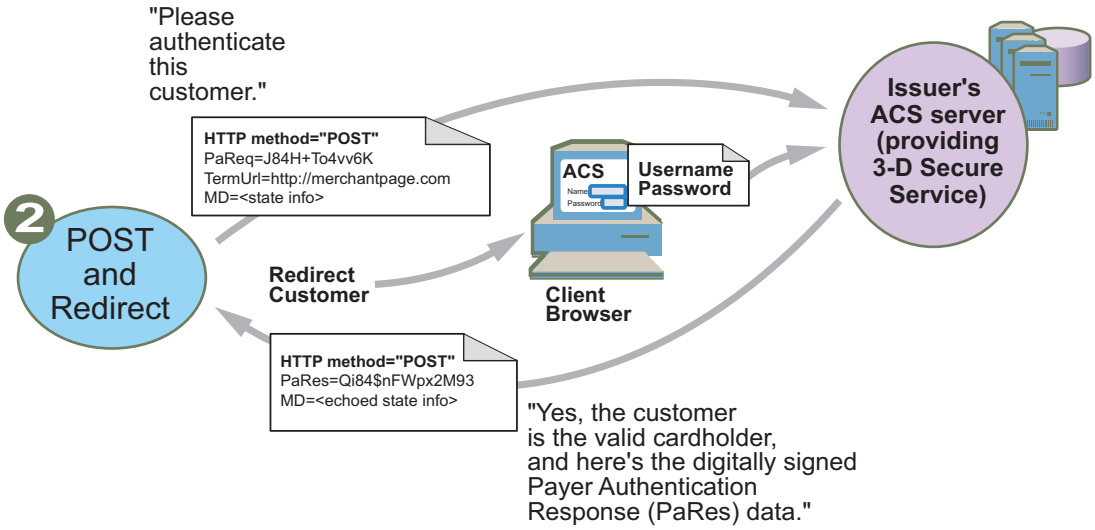
- PAREQ: The value of the PAREQ returned in the Verify Enrollment call.
- TermUrl: Your server—the one that should accept the authentication response.
- MD: (Required) Any data that you want returned (echoed) to the TermUrl by the ACS server. Typically, this is state information.

(XMLPay uses the ValidateAuthentication transaction for this purpose.)

Your server then redirects the customer's browser to the ACS URL.

The customer views the ACS form, enters their 3-D Secure password, and submits the form to the Issuing bank.

The issuer's ACS server validates the password, authenticates the customer's identity, and then generates and digitally signs a PARES value (payer authentication response). The ACS server then HTTP POSTs the signed PARES and the unchanged value of the MD to the TermUrl that you specified.



Example ACS Redirect Code

The following example HTML page redirects a customer to an ACS URL with a PAREQ and returns the URL for receiving the PARES. Customize tags marked with $ with your information.

```
<HTML>
     <head>
     <title>Authentication Body</title>
        <SCRIPT LANGUAGE="Javascript">
           function OnLoadEvent()
           {
              document.downloadForm.submit();
           }
        </SCRIPT>
     </head>

     <body bgcolor="{$BACKCOLOR}" background="{$BACKGROUND}"
        onload="OnLoadEvent()">
        <form name="downloadForm" action="{$acsUrl}" method="POST">
           <noscript>
              <br/>
              <br/>
              <center>
                 <h1>Processing your 3-D Secure Transaction</h1>
                 <h2>JavaScript is currently disabled or is not supported
by your
                    browser.<br/></h2>
```

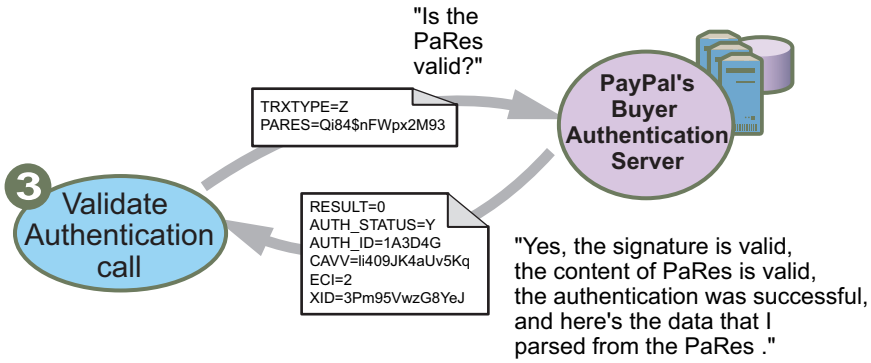
```
                    <h3>Click <b>Submit</b> to continue processing your 3-D
Secure
                       transaction.</h3>
                    <input type="submit" value="Submit"/>
                </center>
            </noscript>

            <input type="hidden" name="TermUrl" value="{$redirectUrl}"/>
            <input type="hidden" name="MD" value="{$messageId}"/>
            <input type="hidden" name="PAREQ" value="{$paReq}"/>
        </form>
    </body>
</HTML>
```

Call 3: Validate the PARES authentication data returned by the ACS server

Your application at TermUrl performs the Validate Authentication call for security reasons. You validate that the PARES is the proper data from the Issuer by sending a request for validation of the digital signature on the PARES to the Buyer Authentication server. Use TRXTYPE=Z.

The server uses the Issuer's digital certificate to validate the signature and then returns the parsed authentication information from the PARES: AUTHENTICATION_STATUS (Y means valid signature), AUTHENTICATION_ID, CAVV (cardholder authentication verification value), XID, and ECI.



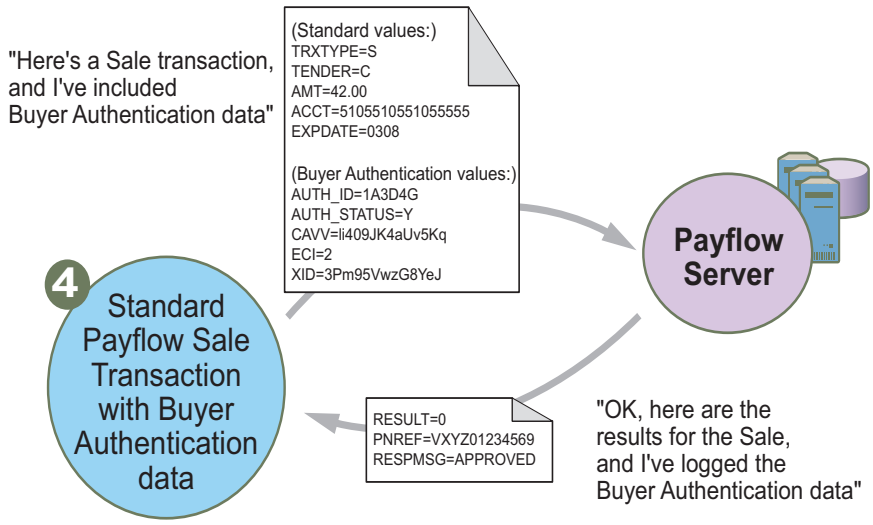
Call 4: Submit the intended transaction request to the Payflow server

NOTE: For Call 4 when using XMLPay, pass the following in ExtData for Authorization and Sale transactions:

AUTHENTICATION_STATUS=<status>, AUTHENTICATION_ID=<id>, CAVV=<cavv value>, and XID=<xid value>, ECI=<eci value>.

Now that when the buyer authentication process is complete, you submit the intended sale or authorization payment transaction (TRXNTYPE=S or A) to the Payflow server. In addition to

the standard sale or authorization transaction data, you include buyer authentication data, as follows:



Cardholder is Enrolled in the 3-D Secure Program

You perform the intended Payflow authorization or sale payment transaction using the standard name-value pairs plus the values returned to the Validate Authentication transaction: AUTHENTICATION_ID, AUTHENTICATION_STATUS, CAVV, XID, and final ECI.

Cardholder is Not Enrolled

If there is no PAREQ returned in the response to the Verify Enrollment call, then the cardholder is not enrolled and you do not perform any additional buyer authentication transactions. You perform the intended Payflow authorization or sale payment transaction using the standard name-value pairs plus the AUTHENTICATION_ID, AUTHENTICATION_STATUS, and ECI values returned by the Verify Enrollment call.

XMLPay Users: Pass AUTHENTICATION_STATUS=<status>, AUTHENTICATION_ID=<id>, CAVV=<cavv value>, XID=<xid value>, and ECI=<eci value> in the ExtData for Authorization and Sale transactions.

Example Buyer Authentication Transactions

The values returned in the transaction responses shown in these examples are described in "Buyer Authentication Transaction Parameters and Return Values" on page 40. Standard Payflow return values are described in *Payflow Pro Developer's Guide*.

All return parameter names for transactions with the Buyer Authentication Server include length tags. Length tags specify the exact number of characters and spaces that appear in the value. For example, RESPMSG[2]=OK.

Example Verify Enrollment Transaction

Use TRXTYPE=E to submit a Verify Enrollment request transaction. The following is an example name-value pair parameter string.

```
"TRXTYPE=E&ACCT=5105105105105100&AMT=19.25&CURRENCY=840&EXPDATE=1206&PARTNE
R=PayPal&PWD=p12345&VENDOR=SuperMerchant&USER=SuperMerchant"
```

Example Verify Enrollment Response

If the cardholder is enrolled, the verify enrollment response contains PAREQ and ACSURL parameters. These are used to direct the cardholder to their Issuer Web site to perform authentication.

Cardholder is enrolled in 3-D Secure program

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=f43669e4921cf8b504c4&AUTHEN
TICATION_STATUS[1]=E&PAREQ[428]=eJxVku1ugjAUhm+FeAH0A3Bozpr48WP+2GK23UA9HJV
ECpYy9e7XCkzXkPS8fcvD6Vvg+2iJ1l+EnSUF79S2+kBRWbxO9mkync4onUmB+3yX8RTTiYLt4p
POCn7ItmVtlIh5LIGN0hMsHrVxCjSel5sPJcMANiioyG7WSgwDWK/B6IrUkloXrfTpVJqDn20Rr
eqq0eYG7O4D1p1x9qbylAMbBXT2pI7ONXPGLpdLvPMU7CHoGTHWFbCwB9ijuW0XqtYzr2Whpi+5
FEWOlGOWU06U7f0HggOFdqQk5wmXIokEn3M5T1Jg93XQVWhCiVksM3/GXkET4IvRCs7zCvioLRk
cjzEqoGtTG/I7fFx/NRTUom99mB59r95CxOh8epngzw8Pad+NgLSKJ6InWg8Ir7HhDtlw3b769x
v8AhQarWM=&ACSURL[66]=http://pilot-buyerauth.-
post.verisign.com/DDDSecure/Acs3DSecureSim/start
```

Cardholder is not enrolled

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=48c92770755039d6bb3d&AUTHEN
TICATION_STATUS[1]=O&ECI[1]=1
```

Example Validate Authentication Transaction

Use TRXTYPE=Z to submit a Validate Authentication transaction to validate the Issuer's digital signature on the PARES, validate the content of the PARES, and to parse the PARES. The following is an example name-value pair parameter string.

NOTE: Ensure that you include no stray carriage returns with the PARES value, especially at the end of the string.

```
"TRXTYPE=Z&PARTNER=PayPal&PWD=p12345&VENDOR=SuperMerchant&USER=SuperMerchan
t&PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQUrWYU3NllEUUBAfv0kWl1l91TPX
ebhTowRBpmHkyfPfr5gbiRlFHF6FFzKaDFXoqry4uhTGn77PAvH4SQKp1MvmEbTnYcf4efF/AVo
UXVj2HD7XjWCzskU0slkGrG33TzqTsUxwhz0nHhbz4l35U7ecfHPh9/dnIE6N7aLeZ0ePlTqRp9
XtVdfqo
...
oZbuHePyp/FUqxyFTXlgV5I/+jMqjde/12HNLjbqW/Qqgfe7Qw9GjcKgt2OdvtTspJPI2eyuRw0
nbr9JKdp6eVP1u3xUyaKN1qYzVksB9vKCe6kqRlV4qfUJP1jvSWl9OKuSbn5zpK0ouzXl9mNfoA
RhDv30qIt+8n719Wbh9fb5+Eh++Fj5+K/wWCuWQ"
```

Example Validate Authentication Response

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6d&AUTHEN
TICATION_STATUS[1]=Y&CAVV[28]=OTJlMzViODhiOTllMjBhYmVkMGU=&ECI[1]=5&XID[28]
=YjM0YTkwNGFkZTI5YmZmZWE1ZmY
```

Displaying the ACS Form

The Issuer ACS page presents transaction information to the cardholder. Visa/MasterCard require that the HTML page for displaying the ACS form must be presented in an in-line frame set. This window must occur within the same browser session as your e-commerce transaction.

The window should have the following browser-independent attributes:

width=390 (minimum), height=400 (minimum), resizable=no, scrollbars=yes, toolbar=no, location=no, directories=no, status=yes, menubar=no

Example Payflow Authorization or Sale Transaction

The Buyer Authentication Service supports only Authorization and Sale transaction types.

The name-value pairs that you submit with the intended Payflow transaction depend upon whether the cardholder is enrolled in the 3-D Secure program, as follows:

Cardholder Enrolled in 3-D Secure Program

You perform the intended transaction using the standard name-value pairs plus the values returned to the Validate Authentication transaction: AUTHENTICATION_ID, AUTHENTICATION_STATUS, CAVV, XID, and ECI. The following is an example name-value pair parameter string.

```
"TRXTYPE=S&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant&USER=SuperMerchant&
PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00&AUTHENTICATION_ID[
20]=8d4d5ed66ac6e6faac6d&CAVV[28]=OTJlMzViODhiOTllMjBhYmVkMGU=&AUTHENTICATI
ON_STATUS[1]=1&ECI[1]=5&XID[28]=YjM0YTkwNGFkZTI5YmZmZWE1ZmY"
```

Cardholder Not Enrolled

If there is no PAREQ returned in the response to the Verify Enrollment call, then the cardholder is not enrolled. You perform the intended transaction using the standard name-value pairs plus the AUTHENTICATION_ID, AUTHENTICATION_STATUS, and ECI returned by the Verify Enrollment transaction. The following is an example name-value pair parameter string.

```
"TRXTYPE=S&TENDER=C&PARTNER=PayPal&VENDOR=SuperMerchant&USER=SuperMerchant&
PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&AMT=123.00&AUTHENTICATION_ID[
20]=8d4d5ed66ac6e6faac6d&AUTHENTICATION_STATUS[1]=O&ECI[1]=7&"
```

Example Payflow Authorization or Sale Transaction Response

For Visa transactions, the response includes a CARDSECURE value of Y (card issuer judges CAVV to be valid), N (card issuer judges CAVV to be invalid), or X (cannot determine validity of CAVV).

- **CAVV Is Valid**

  ```
  RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&A
  VSZIP=N&IAVS=Y&CVV2MATCH=Y&CARDSECURE=Y
  ```

- **CAVV Is Invalid**

  ```
  RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&A
  VSZIP=N&IAVS=Y&CVV2MATCH=Y&CARDSECURE=N
  ```

Buyer Authentication Transaction Parameters and Return Values

The Buyer Authentication server accepts the parameters listed in this section. This section also describes expected return values for buyer authentication transactions.

NOTE: Be sure to follow the guidelines for specifying the parameters. Standard Payflow parameters, parameters that you can pass for reporting purposes, as well as return values are described in *Payflow Pro Developer's Guide*.

Transaction Parameters

In the following tables, ANS indicates alphanumeric-special characters—the set of alphanumeric characters plus characters like / = + : %.

Verify Enrollment Transaction Name-Value Pairs

TABLE 6.2 Verify enrollment parameters

Name	Description	Type	Max. Length
TRXTYPE	E		1
VENDOR	Vendor name		
USER	User name		
PARTNER	Partner name		
PWD	Vendor's password		
ACCT	PAN, card number		
EXPDATE	Expiration mmyy		
AMT	Decimal Amount		

TABLE 6.2 Verify enrollment parameters

Name	Description	Type	Max. Length
CURRENCY	Required ISO 3-number Currency Code (The code for US dollars is 840)		
PUR_DESC	Optional purchase description		

Verify Enrollment Return Values

TABLE 6.3 Verify Enrollment response values

Name	Description	Type	Max. Length
RESULT	0: successful transaction, otherwise error. See "RESULT Codes and RESPMSG Values" on page 68.	integer	1
RESPMSG	Error description if result is not 0. See "RESULT Values for Transaction Declines or Errors" on page 46.	ANS	256
AUTHENTICATION_ID	Unique identifier for this VE event. Value returned only for valid requests.	ANS	64
AUTHENTICATION_STATUS	Value returned only for valid requests. E: Card Enrolled O: Card Not Enrolled X: Unable to determine I: Verify Enrollment request failed	alpha	1
PAREQ	PAREQ. Value returned only if AUTHENTICATION _STATUS=E.	ANS	1024
ACSURL	ACS URL. Value returned only if AUTHENTICATION_ STATUS=E.	ANS	256
ECI	Initial ECI value returned. Value returned only for valid requests.	integer	1

Validate Authentication Transaction Name-Value Pairs

TABLE 6.4 Validate Authentication parameters

Name	Description	Type	Max. Length
TRXTYPE	Z	alpha	1
VENDOR	Vendor name		
USER	User name		
PARTNER	Partner name		
PWD	Merchant's password		
PARES	The complete XML PARES message generated by the ACS		

Validate Authentication Return Values

TABLE 6.5 Validate Authentication response values

Name	Value	Type	Max Length
RESULT	0: successfully verified	integer	1
RESPMSG	Error description if result is not 0	ANS	256
AUTHENTICATION_ID	Message ID of the response, passed with the authorization transaction	ANS	64
AUTHENTICATION_STATUS	The status of the PARES: Y: Authentication Successful — the password was correct. A: Authentication Attempted — the issuing bank does not support buyer authentication N: Authentication Failed (bad password) U: Unable to Authenticate (network error) F: Validate Authentication transaction error	alpha	1
CAVV	CAVV value returned if AUTHENTICATION_Status is Y or A	ANS	64

TABLE 6.5 Validate Authentication response values

Name	Value	Type	Max Length
XID	Transaction ID returned if AUTHENTICATION_Status is Y or A	ANS	64
ECI	ECI if the ECI value is returned in the PARES: 1 - Cardholder not Authenticated (MasterCard) 2 - Cardholder Authenticated (MasterCard) 5 - Authentication Successful (Visa) 6 - Authentication Attempted (Visa) 7 - Authentication Unsuccessful (Visa)	integer	1

Standard Payflow Sale or Authorization Transaction

In addition to the parameters described in *Payflow Pro Developer's Guide*, you submit the following parameters that are specific to the buyer authentication functionality:

TABLE 6.6 Additional Buyer Authentication Sale or Authorization parameters

Name	Value
AUTHENTICATION_ID	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the AUTHENTICATION_ID value returned by the Validate Authentication call. Otherwise, submit the AUTHENTICATION_ID value returned by the Verify Enrollment call.
AUTHENTICATION_STATUS	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the AUTHENTICATION_STATUS value returned by the Validate Authentication call. Otherwise, submit the AUTHENTICATION_STATUS value returned by the Verify Enrollment call.
XID	XID value returned by the Validate Authentication call (if applicable).
ECI	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the ECI value returned by the Validate Authentication call. Otherwise, submit the ECI value returned by the Verify Enrollment call.
CAVV	CAVV value. Returned if AUTHENTICATION_Status is Y or A.

Sale or Authorization Response Value

Visa only: In addition to the return values described in *Payflow Pro Developer's Guide*, the following value is returned:

TABLE 6.7 Buyer Authentication Visa response values

Name	Value
CARDSECURE	Visa only. CAVV validity. Y=Card issuer judges CAVV to be valid N=Card issuer judges CAVV to be invalid X=Cannot determine validity

ECI Values

TABLE 6.8 ECI values

Description of Scenario	Merchant Region	Response to TRXNTYPE=E	Response to TRXNTYPE=X	ECI	Merchant calculates ECI because cannot authenticate?
Visa - Not Enrolled	USA	O	N/A	6	Y
Visa - Unable to determine enrollment	USA	X	N/A	7	Y
Visa - Verify Enrollment transaction error	USA	I	N/A	7	Y
Visa - Card Enrolled - Successful Authentication	USA	E	Y	5	N
Visa - Card Enrolled - Authentication Attempted	USA	E	A (Contact Visa to verify that this value is returned.)	6	N
Visa - Card Enrolled - Authentication Failed	USA	E	N	7	Y
Visa - Card Enrolled - Unable to Authenticate	USA	E	U	7	Y
Visa - Card Enrolled - Error in transaction	USA	E	F	7	Y
MasterCard - Not Enrolled	WORLD	O	N/A	1	Y
MasterCard - Unable to determine enrollment	WORLD	X	N/A	1	Y
MasterCard - Verify enrollment transaction error	WORLD	I	N/A	1	Y
MasterCard - Card Enrolled - Successful Authentication	WORLD	E	Y	2	Y
MasterCard - Card Enrolled - Authentication Attempted	WORLD	E	A (should never occur)	1	Y
MasterCard - Card Enrolled - Authentication Failed	WORLD	E	N	1	Y
MasterCard - Card Enrolled - Unable to Authenticate	WORLD	E	U	1	Y
MasterCard - Card Enrolled - Validation Failed	WORLD	E	F	1	Y

RESULT Values for Transaction Declines or Errors

A RESULT value greater than zero indicates a decline or error. For this type of error, a RESPMSG name-value pair is included. The exact wording of the RESPMSG may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

TABLE 6.9 Buyer Authentication transaction decline or error RESULT values

RESULT	RESPMSG/Explanation
1001	Buyer Authentication Service unavailable
1002	Buyer Authentication Service — Transaction timeout
1003	Buyer Authentication Service — Invalid client version
1004	Buyer Authentication Service — Invalid timeout value
1011	Buyer Authentication Service unavailable
1012	Buyer Authentication Service unavailable
1013	Buyer Authentication Service unavailable
1014	Buyer Authentication Service — Merchant is not enrolled for Buyer Authentication Service (3-D Secure). To enroll, log in to PayPal Manager, click Security, and then click the Buyer Authentication Service banner on the page.
1021	Buyer Authentication Service — Invalid card type
1022	Buyer Authentication Service — Invalid or missing currency code
1023	Buyer Authentication Service — Merchant status for 3D secure is invalid
1041	Validate Authentication failed: missing or invalid PARES
1042	Validate Authentication failed: PARES format invalid
1043	Validate Authentication failed: Cannot find successful Verify Enrollment
1044	Validate Authentication failed: Signature validation failed for PARES
1045	Validate Authentication failed: Mismatched or invalid amount in PARES
1046	Validate Authentication failed: Mismatched or invalid acquirer in PARES
1047	Validate Authentication failed: Mismatched or invalid Merchant ID in PARES
1048	Validate Authentication failed: Mismatched or invalid card number in PARES
1049	Validate Authentication failed: Mismatched or invalid currency code in PARES
1050	Validate Authentication failed: Mismatched or invalid XID in PARES
1051	Validate Authentication failed: Mismatched or invalid order date in PARES
1052	Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction

Logging Transaction Information

A record is maintained of all transactions executed on your account. Use PayPal Manager to view the record and use the information to help reconcile your accounting records.

NOTE: This record is not the official bank statement. The activity on your account is the official record.

In addition, it is strongly recommended that you log all transaction results (except for check information) on your own system. At a minimum, log the following data:

- PNREF (called the Transaction ID in PayPal Manager reports)
- Transaction Date
- Transaction Amount

If you have any questions regarding a transaction, use the PNREF to identify the transaction.

Audit Trail and Transaction Logging

The Buyer Authentication server logs Verify-Enrollment transactions, PAREQ values, and PARES values.

Verify Enrollment Transactions

Verify Enrollment transactions are logged when all of the following items occur:

- The merchant passes data needed to perform buyer authentications.
- The server connects to Visa or MasterCard and gets a meaningful response (card enrollment AUTHENTICATION_STATUS=E, U, or X). If status is Y, then the PAREQ value is logged along with the Verify Enrollment transaction data.

Otherwise, the transaction is not logged.

Validate Authentication Transactions

The Buyer Authentication server will log the PARES value only when all of the following items occur:

- There is a matching PAREQ (by Message ID, not by content) in the database.
- There is no other PARES with the same Message ID in the database. This means that if a duplicate PARES is submitted, it is logged only once.

7 Screening Transactions Using the Payflow SDK

This chapter describes the process of using the Payflow SDK to perform transactions that will be screened by the Fraud Protection Services filters. For information on using the SDK, and on transaction syntax, see *Payflow Pro Developer's Guide*.

IMPORTANT: *Recurring Billing transactions are not screened by Fraud Protection Services filters.*

Response Values. Payflow response values are described in "RESULT Codes and RESPMSG Values" on page 45.

Testing Filters. Information on testing filters appears in Appendix C, "Testing the Transaction Security Filters."

In This Chapter

- "Downloading the Payflow SDK (Including APIs and API Documentation)" on page 29
- "Transaction Parameters Unique to the Filters" on page 32
- "Existing Payflow parameters Used by the Filters" on page 32
- "Response Strings for Transactions that Trigger Filters" on page 34
- "Accepting or Rejecting Transactions That Trigger Filters" on page 40
- "Logging Transaction Information" on page 41

Downloading the Payflow SDK (Including APIs and API Documentation)

The Payflow SDK is available either as a standalone client that can you can integrate with your Web store using CGI scripts or as a set of APIs for direct integration with your application. *Payflow Pro Developer's Guide* The *Payflow Pro Developer's Guide* provides instructions for downloading the SDK appropriate to your platform.

IMPORTANT: *Full API documentation is included with each SDK.*

Transaction Data Required by Filters

This table lists each filter and the Payflow parameter values that are required by the filters.

TABLE 7.1 Parameters required by filter

Filter	**Required Transaction Data**	Payflow **Parameters**
Account Number Velocity	Credit card number	ACCT
AVS Failure	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
Bad Lists	Customer email address	EMAIL
	Credit card number	ACCT
Buyer Auth Failure	You must be enrolled in the Buyer Authentication Services	See Chapter 6, "Performing Buyer Authentication Transactions Using the SDK."
BIN Risk List Match	Credit card number	ACCT
Country Risk List Match	Billing address - country	COUNTRY
	Shipping address - country	COUNTRYCODE
Card Security Code Failure	Card security code information from credit card	CSC
Email Service Provider Risk List	Customer email address	EMAIL
Freight Forwarder Match	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE
	Shipping address - country	COUNTRYCODE

TABLE 7.1 Parameters required by filter

Filter	Required Transaction Data	Payflow **Parameters**
Geo-location Failure	Customer IP address	CUSTIP
	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
	Billing address - state/province	STATE
	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE
Good Lists	Customer email address	EMAIL
	Credit card number	ACCT
International AVS	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
International Shipping/Billing Address	Billing address - country	COUNTRY
	Shipping address - country	COUNTRYCODE
International IP Address	Customer IP address	CUSTIP
IP Address Risk List Match	Customer IP address	CUSTIP
IP Address Velocity	Customer IP address	CUSTIP
Product Watch List	Product SKU or other identifying information	L_SKUn
Shipping/Billing Mismatch*	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
	Billing address - state/province	STATE
	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE

TABLE 7.1 Parameters required by filter

Filter	Required Transaction Data	Payflow **Parameters**
Total Item Ceiling	Total quantity	Total of QTY for all line items within the transaction
Total Purchase Price Ceiling	Total amount	Total of AMT for all line items within the transaction
Total Purchase Price Floor	Total amount	Total of AMT for all line items within the transaction
USPS Address Validation Failure	Billing address - street address	STREET
	Shipping address - street address	SHIPTOSTREET
ZIP Risk List Match	Billing address - ZIP (postal) code	ZIP
	Shipping address - ZIP (postal) code	SHIPTOZIP

Transaction Parameters Unique to the Filters

The Payflow server accepts the parameters listed in this section.

Standard Payflow parameters, parameters that you can pass for reporting purposes, and return values are described in *Payflow Pro Developer's Guide*.

TABLE 7.2 Parameters accepted by the* Payflow *server

Name	Description	Type	Max. Length	Example
BILLTOSTREET2	Extended billing address	Alpha-numeric String	30	Apt. 107
BILLTOPHONE2	Alternative Phone Number for the billing contact.	Numeric String	20	0119120513621, 6104463591
SHIPTOSTREET2	Extended shipping address	String	30	Bldg. 6, Mail Stop 3
SHIPTOPHONE	Primary Phone Number for the shipping contact	String	20	0119120513621, 6104463591
SHIPTOPHONE2	Primary Phone Number for the shipping contact	String	20	0119120513621, 6104463591

TABLE 7.2 Parameters accepted by the Payflow ***server***

Name	Description	Type	Max. Length	Example
SHIPTOEMAIL	Optional. E-mail Address for the shipping contact	String formatted as an email address	40	abc@xyz.com
COUNTRYCODE	Optional. Country code of the shipping country. The country code depends on the processor.	Alpha-numeric String	3	US, USA, 840

Existing Payflow Parameters Used by the Filters

The following existing Payflow parameters (described in *)* are also used by the filters (if they are provided in the transaction request or response):

User Authentication

PARTNER
VENDOR
USER
PWD

Transaction Information

TRXTYPE
TENDER
ACCT
EXPDATE
AMT

Billing Information

FIRSTNAME
MIDDLENAME
LASTNAME
STREET
BILLTOSTREET2
CITY
STATE
ZIP
COUNTRY
PHONENUM
BILLTOPHONE2
EMAIL

Shipping Information

SHIPTOFIRSTNAME
SHIPTOLASTNAME
SHIPTOMIDDLENAME
SHIPTOSTREET
SHIPTOSTREET2
SHIPTOCITY
SHIPTOSTATE
SHIPTOZIP
COUNTRYCODE
SHIPTOPHONE
SHIPTOPHONE2
SHIPTOEMAIL

Order Information

DOB
DL
SS
CUSTIP
BROWSERUSERAGENT
BROWSERTIME
BROWSERCOUNTRYCODE
FREIGHTAMT
TAXAMT
COMMENT1
DESC
CUSTREF
PONUM

Line Item (each item is appended with the line item number)

L_COST0
L_UPC0
L_QTY0
L_DESC0
L_SKU0
L_TYPE0

Response Strings for Transactions that Trigger Filters

In the response string to a transaction that triggered filters, you have the option to view either a summary statement or a detailed list of each triggered filter's response. The response depends on your setting for the VERBOSITY parameter in the transaction request.

- **VERBOSITY=LOW**: This is the default setting for Payflow Pro accounts. The following values (described in *Payflow Pro Developer's Guide*) are returned: {RESULT, PNREF, RESPMSG, AUTHCODE, AVSADDR, AVSZIP, CVV2MATCH, IAVS, CARDSECURE}

  The following values are specific to Fraud Protection Services:

TABLE 7.3 Low VERBOSITY parameters

Parameter	Description
RESULT	See "RESULT Values Specific to Fraud Protection Services" on page 37.
PREFPSMSG	Preprocessing Fraud Protection Services messages. These apply to all filters except: AVS Failure, Card Security Code Failure, and Custom Filters.
POSTFPSMSG	Postprocessing Fraud Protection Services messages. These apply to the following filters only: AVS Failure, Card Security Code Failure, and Custom Filters.

- **VERBOSITY=MEDIUM**: Returns all of the values returned for a LOW setting, plus the following values:

TABLE 7.4 Medium VERBOSITY parameters

Parameter	Type	Length	Description
FPS_PREXMLDATA	char		Itemized list of responses for triggered filters.
HOSTCODE	char	7	Response code returned by the processor. This value is not normalized.
RESPTEXT	char	17	Text corresponding to the response code returned by the processor. This text is not normalized.
PROCAVS	char	2	AVS (Address Verification Service) response from the processor
PROCCVV2	char	1	CVV2 (buyer authentication) response from the processor
PROCCARDSECURE	char	1	VPAS/SPA response from the processor
ADDLMSGS	char	Up to 1048 characters. Typically 50 characters.	Additional error message that indicates that the merchant used a feature that is disabled

TABLE 7.4 Medium VERBOSITY parameters

Parameter	Type	Length	Description
TRANSSTATE	Integer	10	State of the transaction. The values are: 0 = General succeed state 1 = General error state 3 = Authorization approved 6 = Settlement pending (transaction is scheduled to be settled) 7 =Settlement in progress (transaction involved in a currently ongoing settlement) 8 = Settled successfully 9 = Authorization captured (once an authorization type transaction is captured, its TRANSSTATE becomes 9) 10 =Capture failed (an error occurred while trying to capture an authorization because the transaction was already captured) 11 = Failed to settle (transactions fail settlement usually because of problems with the merchant's processor or because the card type is not set up with the merchant's processor) 12 - Unsettled transaction because of incorrect account information 14 = For various reasons, the batch containing this transaction failed settlement 16 = Merchant ACH settlement failed; (need to manually collect it). For information on TRANSSTATE incremental values, see the table below.
DATE_TO_SETTLE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only before settlement has started.

TABLE 7.4 Medium VERBOSITY parameters

Parameter	Type	Length	Description
BATCHID	Integer	10	Value available only after settlement has assigned a Batch ID.
SETTLE_DATE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only after settlement has completed.

NOTE: If you use Nashville, TeleCheck, or Paymentech, then you must use a client version newer than 2.09 to take advantage of the MEDIUM verbosity setting. For information on interpreting the responses returned by the processor for the MEDIUM Verbosity setting, contact your processor directly.

The table below shows the increments that are possible on basic TRANSSTATE values.

TABLE 7.5 TRANSSTATE value increments

Increment	Meaning
+100	No client acknowledgment (ACK) is received (=status 0 in V2), for example, 106 is TRANSSTATE 6.
+200	The host process never receives ACK from the transaction broker (or backend payment server). A transaction with a TRANSSTATE of +200 is basically in limbo and will not be settled.
+1000	Voided transactions. Any TRANSSTATE of +1000 (for example, 1006) means the transaction was settle pending. However, it was voided either through the API PayPal Manager, or Customer Service.

RESULT Values Specific to Fraud Protection Services

A RESULT value greater than zero indicates a decline or error. For this type of error, a RESPMSG name-value pair is included. The exact wording of the RESPMSG may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

TABLE 7.6 Transaction RESULTs/RESPMSGs

RESULT	RESPMSG and Explanation
125	Fraud Protection Services Filter — Declined by filters
126	Fraud Protection Services Filter — Flagged for review by filters
127	Fraud Protection Services Filter — Not screened by filters

TABLE 7.6 Transaction RESULTs/RESPMSGs *(Continued)*

RESULT	RESPMSG and Explanation
128	Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters
131	Version 1 Payflow client no longer supported. Upgrade to the most recent version of the Payflow client.

Changing the Verbosity Setting

Setting the default verbosity level for all transactions

Contact Customer Service to set your account's verbosity setting to `LOW` or `MEDIUM` for all transaction requests.

Setting the verbosity level on a per-transaction basis

To specify a setting for verbosity that differs from your account's current setting, include the `VERBOSITY=<value>` name-value pair in the transaction request, where `<value>` is `LOW` or `MEDIUM`.

NOTE: In the examples below, the <action> tag value is the state to which the transaction has been set. Values are: R = Review, J = Reject, A = Accept.

Example Response for an Authentication Transaction With Verbosity=Low

```
RESULT=126&PNREF=VFHA28926593&RESPMSG=Under review by Fraud
Service&AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCODE=A&PROCAVS=A
&PROCCVV2=X&IAVS=N&PREFPSMSG=Review: More than one rule was triggered for
Review&POSTFPSMSG=Review: More than one rule was triggered for Review
```

Example Response for an Authentication Transaction With Verbosity=Medium

```
RESULT=126(0)&PNREF=VFHA28926593&RESPMSG=Under review by Fraud
Service(Approved)&AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCODE=A
&PROCAVS=A&PROCCVV2=X&IAVS=N&PREFPSMSG=Review: More than one rule was
triggered for Review&FPS_PREXMLDATA[2898]=<triggeredRules><rule
num="1"><ruleId>2</ruleId><ruleAlias>CeilingAmount</ruleAlias><ruleDescript
ion>Total Purchase Price
Ceiling</ruleDescription><action>R</action><triggeredMessage>The purchase
amount of 7501 is greater than the ceiling value set of
7500</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>CeilingValue</name><value
type="USD">75.00</value></ruleParameter></rulevendorparms></rule><rule
num="2"><ruleId>6</ruleId><ruleAlias>HighOrderNumber</ruleAlias><ruleDescri
```

ption>Total
ItemCeiling</ruleDescription><action>R</action><triggeredMessage>16 items
were ordered, which is over the maximum allowed quantity of
15</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><valuetype="Integer">15</value></ruleParameter></
rulevendorparms></rule>(Remove text
completely<rulenum="3"><ruleId>7</ruleId><ruleAlias>BillShipMismatch</ruleA
lias><ruleDescription>Shipping/BillingMismatch</ruleDescription><action>R</
action><triggeredMessage>The billing and shipping addresses did not
match</triggeredMessage></rule><rulenum="4"><ruleId>13</ruleId><ruleAlias>H
ighRiskBinCheck</ruleAlias><ruleDescription>BIN Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The card number
is in a high risk bin
list</triggeredMessage></rule><rulenum="5"><ruleId>37</ruleId><ruleAlias>Hi
ghRiskZIPCheck</ruleAlias><ruleDescription>Zip Risk List
Match</ruleDescription><action>R</action><triggeredMessage>High risk
shipping
zip</triggeredMessage></rule><rulenum="6"><ruleId>16</ruleId><ruleAlias>Bil
lUSPostalAddressCheck</ruleAlias><
ruleDescription>USPS Address Validation
Failure</ruleDescription><action>R</action><triggeredMessage>The billing
address is not a valid US
Address</triggeredMessage><rulevendorparms><ruleParameternum="1"><name>Addr
essToVerify</name><valuetype="String">bill</value></ruleParameter></ruleven
dorparms></rule>(Remove text
completely)<rulenum="7"><ruleId>10</ruleId><ruleAlias>HighRiskEmailCheck</r
uleAlias><ruleDescription>Email Service Provider Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The email
address fraud@asiamail.com in bill Email was found in a high risk email
providerlist</triggeredMessage></rule><rulenum="8"><ruleId>38</ruleId><rule
Alias>GeoLocationCheck</ruleAlias><ruleDescription>Geo-Location
Failure</ruleDescription><action>R</action><triggeredMessage>GeoLocation
difference: Bill Address and IP, GeoLocation difference: Ship Address and
IP</triggeredMessage></rule><rulenum="9"><ruleId>8</ruleId><ruleAlias>NonUS
IPAddress</ruleAlias><ruleDescrip tion>International IP
Address</ruleDescription><action>R</action><triggeredMessage>The IP address

```
is from:
CZ</triggeredMessage></rule><rulenum="10"><ruleId>41</ruleId><ruleAlias>Hig
hRiskFreightCheck</ruleAlias><ruleDescription>Freight Forwarder
Match</ruleDescription><action>R</action><triggeredMessage>High riskg
freight forwarder</triggeredMessage></rule>(Remove text
completely</triggeredRules>&POSTFPSMSG=Review:More than one rule was
triggered for
Review&FPS_POSTXMLDATA[682]=<triggeredRules><rulenum="1"><ruleId>1</ruleId>
<ruleAlias>AVS</ruleAlias><ruleDescription>AVS
Failure</ruleDescription><action>R</action><triggeredMessage>AVS check
failed: Full
Security</triggeredMessage><rulevendorparms><ruleParameternum="1"><name>Val
ue</name><valuetype="String">Full</value></ruleParameter></rulevendorparms>
</rule>(Remove text
completely)<rulenum="2"><ruleId>23</ruleId><ruleAlias>CSCFailure</ruleAlias
><ruleDescription>CSC
Failure</ruleDescription><action>R</action><triggeredMessage>CSC check
failed, returned
X</triggeredMessage><rulevendorparms><ruleParameternum="1"><name>Value</nam
e><valuetype="String">Full</value></ruleParameter></rulevendorparms></rule>
</triggeredRules>
```

RESULT=126&PNREF=VFHA28926593&RESPMSG=Under review by Fraud
Service&AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCODE=A&PROCAVS=A
&PROCCVV2=X&IAVS=N&PREFPSMSG=Review: More than one rule was triggered for
Review&FPS_PREXMLDATA[2898]=<triggeredRules><rule
num="1"><ruleId>2</ruleId><ruleAlias>CeilingAmount</ruleAlias><ruleDescript
ion>Total Purchase Price
Ceiling</ruleDescription><action>R</action><triggeredMessage>The purchase
amount of 7501 is greater than the ceiling value set of
7500</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>CeilingValue</name><value
type="USD">75.00</value></ruleParameter></rulevendorparms></rule><rule
num="2"><ruleId>6</ruleId><ruleAlias>HighOrderNumber</ruleAlias><ruleDescri
ption>Total Item
Ceiling</ruleDescription><action>R</action><triggeredMessage>16 items were
ordered, which is over the maximum allowed quantity of
15</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="Integer">15</value></ruleParameter></rulevendorparms></rule><rule
num="3"><ruleId>7</ruleId><ruleAlias>BillShipMismatch</ruleAlias><ruleDescr
iption>Shipping/Billing
Mismatch</ruleDescription><action>R</action><triggeredMessage>The billing
and shipping addresses did not match</triggeredMessage></rule><rule
num="4"><ruleId>13</ruleId><ruleAlias>HighRiskBinCheck</ruleAlias><ruleDesc
ription>BIN Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The card number
is in a high risk bin list</triggeredMessage></rule><rule
num="5"><ruleId>37</ruleId><ruleAlias>HighRiskZIPCheck</ruleAlias><ruleDesc
ription>Zip Risk List
Match</ruleDescription><action>R</action><triggeredMessage>High risk
shipping zip</triggeredMessage></rule><rule
num="6"><ruleId>16</ruleId><ruleAlias>BillUSPostalAddressCheck</ruleAlias><
ruleDescription>USPS Address Validation
Failure</ruleDescription><action>R</action><triggeredMessage>The billing
address is not a valid US
Address</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>AddressToVerify</name><value
type="String">bill</value></ruleParameter></rulevendorparms></rule><rule
num="7"><ruleId>10</ruleId><ruleAlias>HighRiskEmailCheck</ruleAlias><ruleDe
scription>Email Service Provider Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The email
address fraud@asiamail.com in billEmail was found in a high risk email
provider list</triggeredMessage></rule><rule
num="8"><ruleId>38</ruleId><ruleAlias>GeoLocationCheck</ruleAlias><ruleDesc
ription>Geo-Location
Failure</ruleDescription><action>R</action><triggeredMessage>GeoLocation
difference: Bill Address and IP, GeoLocation difference: Ship Address and
IP</triggeredMessage></rule><rule
num="9"><ruleId>8</ruleId><ruleAlias>NonUSIPAddress</ruleAlias><ruleDescrip
tion>International IP
Address</ruleDescription><action>R</action><triggeredMessage>The IP address
is from: CZ</triggeredMessage></rule><rule

```
num="10"><ruleId>41</ruleId><ruleAlias>HighRiskFreightCheck</ruleAlias><rul
eDescription>Freight Forwarder
Match</ruleDescription><action>R</action><triggeredMessage>High risk
freight
forwarder</triggeredMessage></rule></triggeredRules>&POSTFPSMSG=Review:
More than one rule was triggered for
Review&FPS_POSTXMLDATA[682]=<triggeredRules><rule
num="1"><ruleId>1</ruleId><ruleAlias>AVS</ruleAlias><ruleDescription>AVS
Failure</ruleDescription><action>R</action><triggeredMessage>AVS check
failed: Full Security</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="String">Full</value></ruleParameter></rulevendorparms></rule><rule
num="2"><ruleId>23</ruleId><ruleAlias>CSCFailure</ruleAlias><ruleDescriptio
n>CSC Failure</ruleDescription><action>R</action><triggeredMessage>CSC
check failed, returned X</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="String">Full</value></ruleParameter></rulevendorparms></rule></trigge
redRules>
```

Accepting or Rejecting Transactions That Trigger Filters

You can submit a transaction request that either accepts or rejects a transaction that triggered a filter (Result code 126). This is the functional equivalent of the operations discussed in "Acting on Transactions that Triggered Filters" on page 21.

- **Accept**: Submit the transaction for normal processing.
- **Reject**: Do not submit the transaction for processing. See "Rejecting Transactions" on page 23.

NOTE: You must contact Customer Service to enable this feature. Telephone: 1-888-883-9770. E-mail: payflow-support@paypal.com

To accept or reject a transaction, include the following values in the transaction request:

- TRXTYPE=U
- ORIGID=<PNREF returned for the original transaction>
- UPDATEACTION=APPROVE (to accept)

  — or —

  UPDATEACTION=FPS_MERCHANT_DECLINE (to reject)

Logging Transaction Information

A record is maintained of all transactions executed on your account. Use PayPal Manager to view the record and use the information to help reconcile your accounting records.

NOTE: This record is not the official bank statement. The activity on your account is the official record.

In addition, it is strongly recommends that you log all transaction results (except for check information) on your own system. At a minimum, log the following data:

- PNREF (called the **Transaction ID** in PayPal Manager reports)
- Transaction Date
- Transaction Amount

If you have any questions regarding a transaction, use the PNREF to identify the transaction.

8 Responses to Credit Card Transaction Requests

This chapter describes the contents of a response to a credit card transaction request.

In This Chapter

- "An Example Response String" on page 65
- "Contents of a Response to a Credit Card Transaction Request" on page 66
- "PNREF Value" on page 67
- "RESULT Codes and RESPMSG Values" on page 68

An Example Response String

When a transaction finishes, the server returns a response string made up of name-value pairs. For example, this is a response to a credit card **Sale** transaction request:

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&AVSZ
IP=N&IAVS=Y&CVV2MATCH=Y
```

Contents of a Response to a Credit Card Transaction Request

All transaction responses include values for RESULT, PNREF, and RESPMSG. A value for AUTHCODE is included for Voice Authorization transactions. Values for AVSADDR and AVSZIP are included if you use address verification system (AVS). Table 8.1 describes the values returned in a response string.

TABLE 8.1 Transaction response values

Field	Description	Type	Length
PNREF	Reference ID, a unique number that identifies the transaction. PNREF is described in "PNREF Format" on page 67.	Alpha-numeric	12
RESULT	The outcome of the attempted transaction. A result of 0 (zero) indicates the transaction was approved. Any other number indicates a decline or error. RESULT codes are described in "RESULT Codes and RESPMSG Values" on page 68.	Numeric	Variable
CVV2MATCH	Result of the card security code (CVV2) check. The issuing bank may decline the transaction if there is a mismatch. In other cases, the transaction may be approved despite a mismatch.	Alpha Y, N, X, or no response	1
RESPMSG	The response message returned with the transaction result. Exact wording varies. Sometimes a colon appears after the initial RESPMSG followed by more detailed information. Response messages are described in "RESULT Codes and RESPMSG Values" on page 68.	Alpha-numeric	Variable
PPREF	Unique transaction ID of the payment. If the TRXTYPE of the request is A, then you will need the value of PPREF for use with Authorization and Delayed Capture transactions.	string	17
AUTHCODE	Returned for Sale, Authorization, and Voice Authorization transactions. AUTHCODE is the approval code obtained over the phone from the processing network. AUTHCODE is required when submitting a Force (F) transaction.	Alpha-numeric	6
AVSADDR	AVS address responses are for advice only. This process does not affect the outcome of the authorization.	Alpha Y, N, X, or no response	1

TABLE 8.1 Transaction response values *(Continued)*

Field	Description	Type	Length
AVSZIP	AVS ZIP code responses are for advice only. This process does not affect the outcome of the authorization.	Alpha Y, N, X, or no response	1
IAVS	International AVS address responses are for advice only. This value does not affect the outcome of the transaction. Indicates whether AVS response is international (Y), US (N), or cannot be determined (X). Client version 3.06 or later is required.	Alpha Y, N, X, or no response	1

PNREF Value

The PNREF is a unique transaction identification number issued by the server that identifies the transaction for billing, reporting, and transaction data purposes. The PNREF value appears in the Transaction ID column in PayPal Manager reports.

- The PNREF value is used as the ORIGID value (original transaction ID) in delayed capture transactions (TRXTYPE=D), credits (TRXTYPE=C), inquiries (TRXTYPE=I), and voids (TRXTYPE=V).
- The PNREF value is used as the ORIGID value (original transaction ID) value in reference transactions for authorization (TRXTYPE=A) and Sale (TRXTYPE=S).

NOTE: The PNREF is also referred to as the Transaction ID in Payflow Link documentation.

PNREF Format

The PNREF is a 12-character string of printable characters, for example:

- EFHP0D426838
- ACRAF23DB3C4

NOTE: Printable characters also include symbols other than letters and numbers such as the question mark (?). A PNREF typically contains letters and numbers only.

The PNREF in a transaction response tells you that your transaction is connecting to the server.

Historically, the contents of a PNREF indicated a test or a live transaction. However, this is not always the case, and as a rule, you should not place any meaning on the contents of a PNREF.

RESULT Codes and RESPMSG Values

RESULT is the first value returned in the server response string. The value of the RESULT parameter indicates the overall status of the transaction attempt.

- A value of 0 (zero) indicates that no errors occurred and the transaction was approved.
- A value less than zero indicates that a communication error occurred. In this case, no transaction is attempted.
- A value greater than zero indicates a decline or error.

The response message (RESPMSG) provides a brief description for decline or error results.

RESULT Values for Transaction Declines or Errors

For non-zero Results, the response string includes a RESPMSG name-value pair. The exact wording of the RESPMSG (shown in **bold**) may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
0	**Approved.** **NOTE:** PayPal processor: Warning information may be returned that may be useful to the request applicaton. See the PayPal API documentation on the PayPal website for information on corrective actions.
1	**User authentication failed.** Error is caused by one or more of the following: • Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. VENDOR is your merchant ID and USER is the same as VENDOR unless you created a Payflow Pro user. All fields are case sensitive. • Invalid Processor information entered. Contact merchant bank to verify. • "Allowed IP Address" security feature implemented. The transaction is coming from an unknown IP address. See PayPal Manager online help for details on how to use Manager to update the allowed IP addresses. • You are using a test (not active) account to submit a transaction to the live PayPal servers. Change the host address from the test server URL to the live server URL.
2	**Invalid tender type.** Your merchant bank account does not support the following credit card type that was submitted.
3	**Invalid transaction type.** Transaction type is not appropriate for this transaction. For example, you cannot credit an authorization-only transaction.
4	**Invalid amount format. Use the format: "#####.##" Do not include currency symbols or commas.**

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
5	**Invalid merchant information.** Processor does not recognize your merchant account information. Contact your bank account acquirer to resolve this problem.
6	Invalid or unsupported currency code
7	**Field format error.** Invalid information entered. See RESPMSG.
8	**Not a transaction server**
9	**Too many parameters or invalid stream**
10	**Too many line items**
11	**Client time-out waiting for response**
12	**Declined.** Check the credit card number, expiration date, and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call their card issuing bank to resolve.
13	**Referral.** Transaction cannot be approved electronically but can be approved with a verbal authorization. Contact your merchant bank to obtain an authorization and submit a manual Voice Authorization transaction.
14	**Invalid Client Certification ID.** Check the HTTP header. If the tag, X-VPS-VIT-CLIENT-CERTIFICATION-ID, is missing, RESULT code 14 is returned.
19	**Original transaction ID not found.** The transaction ID you entered for this transaction is not valid. See RESPMSG.
20	**Cannot find the customer reference number**
22	**Invalid ABA number**
23	**Invalid account number.** Check credit card number and re-submit.
24	**Invalid expiration date.** Check and re-submit.
25	**Invalid Host Mapping.** You are trying to process a tender type such as Discover Card, but you are not set up with your merchant bank to accept this card type.
26	**Invalid vendor account.** Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. VENDOR is your merchant ID and USER is the same as VENDOR unless you created a Payflow Pro user. All fields are case sensitive.
27	**Insufficient partner permissions**
28	**Insufficient user permissions**
29	**Invalid XML document.** This could be caused by an unrecognized XML tag or a bad XML format that cannot be parsed by the system.
30	**Duplicate transaction**

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
31	**Error in adding the recurring profile**
32	**Error in modifying the recurring profile**
33	**Error in canceling the recurring profile**
34	**Error in forcing the recurring profile**
35	**Error in reactivating the recurring profile**
36	**OLTP Transaction failed**
37	**Invalid recurring profile ID**
50	**Insufficient funds available in account**
51	**Exceeds per transaction limit**
99	**General error.** See RESPMSG.
100	**Transaction type not supported by host**
101	**Time-out value too small**
102	**Processor not available**
103	**Error reading response from host**
104	**Timeout waiting for processor response.** Try your transaction again.
105	**Credit error.** Make sure you have not already credited this transaction, or that this transaction ID is for a creditable transaction. (For example, you cannot credit an authorization.)
106	**Host not available**
107	**Duplicate suppression time-out**
108	**Void error.** See RESPMSG. Make sure the transaction ID entered has not already been voided. If not, then look at the Transaction Detail screen for this transaction to see if it has settled. (The Batch field is set to a number greater than zero if the transaction has been settled). If the transaction has already settled, your only recourse is a reversal (credit a payment or submit a payment for a credit).
109	**Time-out waiting for host response**
110	**Referenced auth (against order) Error**
111	**Capture error.** Either an attempt to capture a transaction that is not an authorization transaction type, or an attempt to capture an authorization transaction that has already been captured.
112	**Failed AVS check.** Address and ZIP code do not match. An authorization may still exist on the cardholder's account.

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
113	**Merchant sale total will exceed the sales cap with current transaction.** ACH transactions only.
114	**Card Security Code (CSC) Mismatch.** An authorization may still exist on the cardholder's account.
115	**System busy, try again later**
116	**VPS Internal error. Failed to lock terminal number**
117	**Failed merchant rule check.** One or more of the following three failures occurred: An attempt was made to submit a transaction that failed to meet the security settings specified on the PayPal Manager *Security Settings* page. If the transaction exceeded the Maximum Amount *security setting,* then no values are returned for AVS or CSC. AVS validation failed. The AVS return value should appear in the RESPMSG. CSC validation failed. The CSC return value should appear in the RESPMSG.
118	**Invalid keywords found in string fields**
119	**General failure within PIM Adapter**
120	**Attempt to reference a failed transaction**
121	**Not enabled for feature**
122	**Merchant sale total will exceed the credit cap with current transaction.** ACH transactions only.
125	**Fraud Protection Services Filter — Declined by filters**
126	**Fraud Protection Services Filter — Flagged for review by filters** **Important Note:** Result code 126 indicates that a transaction triggered a fraud filter. This is not an error, but a notice that the transaction is in a review status. The transaction has been authorized but requires you to review and to manually accept the transaction before it will be allowed to settle. Result code 126 is intended to give you an idea of the kind of transaction that is considered suspicious to enable you to evaluate whether you can benefit from using the Fraud Protection Services. To eliminate result 126, turn the filters off. For more information, see the Fraud Protection Services documentation for your payments solution. It is available on the PayPal Manager Documentation page.
127	**Fraud Protection Services Filter — Not processed by filters**
128	**Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters**
131	**Version 1 Payflow Pro SDK client no longer supported.** Upgrade to the most recent version of the Payflow Pro client.
132	**Card has not been submitted for update**

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
133	**Data mismatch in HTTP retry request**
150	**Issuing bank timed out**
151	**Issuing bank unavailable**
200	**Reauth error**
201	**Order error**
402	**PIM Adapter Unavailable**
403	**PIM Adapter stream error**
404	**PIM Adapter Timeout**
600	**Cybercash Batch Error**
601	**Cybercash Query Error**
1000	**Generic host error.** This is a generic message returned by your credit card processor. The RESPMSG will contain more information describing the error.
1001	**Buyer Authentication Service unavailable**
1002	**Buyer Authentication Service — Transaction timeout**
1003	**Buyer Authentication Service — Invalid client version**
1004	**Buyer Authentication Service — Invalid timeout value**
1011	**Buyer Authentication Service unavailable**
1012	**Buyer Authentication Service unavailable**
1013	**Buyer Authentication Service unavailable**
1014	**Buyer Authentication Service — Merchant is not enrolled for Buyer Authentication Service (3-D Secure).**
1016	**Buyer Authentication Service — 3-D Secure error response received.** Instead of receiving a PARes response to a Validate Authentication transaction, an error response was received.
1017	**Buyer Authentication Service — 3-D Secure error response is invalid.** An error response is received and the response is not well formed for a Validate Authentication transaction.
1021	**Buyer Authentication Service — Invalid card type**
1022	**Buyer Authentication Service — Invalid or missing currency code**
1023	**Buyer Authentication Service — merchant status for 3D secure is invalid**

TABLE 8.2 Payflow transaction RESULT values and RESPMSG text *(Continued)*

RESULT	RESPMSG and Explanation
1041	**Buyer Authentication Service — Validate Authentication failed: missing or invalid PARES**
1042	**Buyer Authentication Service — Validate Authentication failed: PARES format is invalid**
1043	**Buyer Authentication Service — Validate Authentication failed: Cannot find successful Verify Enrollment**
1044	**Buyer Authentication Service — Validate Authentication failed: Signature validation failed for PARES**
1045	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid amount in PARES**
1046	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid acquirer in PARES**
1047	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid Merchant ID in PARES**
1048	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid card number in PARES**
1049	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid currency code in PARES**
1050	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid XID in PARES**
1051	**Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid order date in PARES**
1052	**Buyer Authentication Service — Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction**

RESULT Values for Communications Errors

A RESULT value less than zero indicates that a communication error occurred. In this case, no transaction is attempted.

A value of -1 or -2 usually indicates a configuration error caused by an incorrect URL or by configuration issues with your firewall. A value of -1 or -2 can also be possible if the PayPal servers are unavailable, or an incorrect server/socket pair has been specified. A value of -1 can also result when there are internet connectivity errors. Contact customer support regarding any other errors.

TABLE 8.3 RESULT values for communications errors

RESULT	Description
-1	**Failed to connect to host**
-2	**Failed to resolve hostname**
-5	**Failed to initialize SSL context**
-6	**Parameter list format error: & in name**
-7	**Parameter list format error: invalid [ ] name length clause**
-8	**SSL failed to connect to host**
-9	**SSL read failed**
-10	**SSL write failed**
-11	**Proxy authorization failed**
-12	**Timeout waiting for response**
-13	**Select failure**
-14	**Too many connections**
-15	**Failed to set socket options**
-20	**Proxy read failed**
-21	**Proxy write failed**
-22	**Failed to initialize SSL certificate**
-23	**Host address not specified**
-24	**Invalid transaction type**
-25	**Failed to create a socket**
-26	**Failed to initialize socket layer**
-27	**Parameter list format error: invalid [ ] name length clause**
-28	**Parameter list format error: name**
-29	**Failed to initialize SSL connection**
-30	**Invalid timeout value**
-31	**The certificate chain did not validate, no local certificate found**
-32	**The certificate chain did not validate, common name did not match URL**
- 40	**Unexpected Request ID found in request.**

TABLE 8.3 RESULT values for communications errors*(Continued)*

RESULT	Description
- 41	**Required Request ID not found in request**
-99	**Out of memory**
-100	**Parameter list cannot be empty**
-103	**Context initialization failed**
-104	**Unexpected transaction state**
-105	**Invalid name value pair request**
-106	**Invalid response format**
-107	**This XMLPay version is not supported**
-108	**The server certificate chain did not validate**
-109	**Unable to do logging**
-111	**The following error occurred while initializing from message file: <Details of the error message>**
-113	**Unable to round and truncate the currency value simultaneously**

A Fraud Filter Reference

This appendix describes the filters that make up part of the Fraud Protection Services. Filters analyze transactions and act on those that show evidence of potential fraudulent activity. Filters can set such transactions aside for your review or reject them outright, depending on settings that you specify.

Filters are grouped to help you to assess the risk types and to take action (accept, reject, or continue in the review state).

In This Appendix

- "Filters Included with the Fraud Protection Services" on page 77
- "About the Fraud Risk Lists" on page 78
- "Filters Applied After Processing" on page 79
- "Unusual Order Filters" on page 79
- "High-risk Payment Filters" on page 81
- "High-risk Address Filters" on page 86
- "High-risk Customer Filters" on page 90
- "International Order Filters" on page 91
- "Accept Filters" on page 93
- "Custom Filters" on page 94

Filters Included with the Fraud Protection Services

Fraud Protection Services offers Basic and Advanced options. The filters included with each option are listed here. In addition, the optional **Buyer Authentication Failure** filter is described on page 78.

Filters Included with the Basic Fraud Protection Services Option

- "Total Purchase Price Ceiling Filter" on page 79
- "Total Item Ceiling Filter" on page 80
- "Shipping/Billing Mismatch Filter" on page 80
- "AVS Failure Filter" on page 81
- "Card Security Code Failure Filter" on page 83
- "ZIP Risk List Match Filter" on page 87

- "Freight Forwarder Risk List Match Filter" on page 87
- "IP Address Velocity Filter" on page 90

Filters Included with the Advanced Fraud Protection Services Option

All Basic filters plus:

- "Buyer Authentication Failure Filter" on page 84
- "USPS Address Validation Failure Filter" on page 87
- "Email Service Provider Risk List Match Filter" on page 88
- "IP Address Match Filter" on page 88
- "Account Number Velocity Filter" on page 86
- "Geo-location Failure Filter" on page 89
- "Bad Lists" on page 90
- "International Shipping/Billing Address Filter" on page 91
- "International AVS Filter" on page 92
- "International IP Address Filter" on page 92
- "Country Risk List Match Filter" on page 91
- "Good Lists" on page 93
- "Total Purchase Price Floor Filter" on page 94
- "Custom Filters" on page 94
- "Product Watch List Filter" on page 81

Special Case: Buyer Authentication Failure Filter

The optional Buyer Authentication service is described in "Buyer Authentication Service" on page 10. The **Buyer Authentication Failure** filter, which screens the customer authentication data returned by the service, is described on page 84.

About the Fraud Risk Lists

Filters whose name includes "Risk List" make use of lists that the Fraud Protections Services manage. Extensive statistical analysis of millions of e-commerce transactions is performed to determine transaction data elements (for example BIN numbers or ZIP codes) that are statistically more likely than average to be correlated with fraudulent transactions.

Inclusion in a Risk List is not an absolute indication of fraud, only a statistical correlation that indicates that you should evaluate the transaction more closely (and in conjunction with other filter results for the transaction).

Filters Applied After Processing

Most filters are applied to the transaction request before forwarding the request to the processor. The following filters are applied to the transaction results that the processor returns:

- AVS Failure filter (described on page 81)
- Card Security Code Failure filter (described on page 83)
- International AVS filter (described on page 92)
- Custom filters (described on page 94)

Transaction Data Required by Filters

"Downloading the Payflow SDK (Including APIs and API Documentation)" on page 49 provides the full list, for each filter, of each transaction value that you must send to Payflow Pro. For example, to ensure that the Total Item Ceiling filter can screen an order, you must provide the total number of items that make up the order.

Unusual Order Filters

Unusual Order Filters identify transactions that exceed the normal size for your business. Because fraudsters might not feel limited in their purchasing power, they sometimes place orders that are much larger than the norm.

Total Purchase Price Ceiling Filter

What does the filter do?

This filter compares the total amount of the transaction (including tax, shipping and handling fees) to the maximum purchase amount (the ceiling) that you specify.

The specified action is taken whenever a transaction amount exceeds the specified ceiling.

IMPORTANT: *The Maximum amount per transaction setting in the Account menu controls all transactions, even those that are less than or exceed the Total Purchase Price Ceiling filter.*

How does the filter protect me?

An unusually high purchase amount (compared to the average for your business) can indicate potential fraudulent activity. Because fraudsters are not paying with their own money, they are not price-sensitive.

Total Item Ceiling Filter

What does the filter do?

This filter compares the total number of items (or volume for bulk commodities) to the maximum count (the ceiling) that you specify.

The specified action is taken whenever the item count in a transaction exceeds the specified ceiling.

How does the filter protect me?

An unusually high item count (compared to the average for your business) can indicate potential fraudulent activity. Fraudsters frequently attempt to order large numbers of attractive items that can easily be resold.

NOTE: In addition, some items are more susceptible to fraud than others. For example, a computer can be resold for much more money than can a pair of sport shoes. The likelihood of selling the item quickly is also a factor.

Shipping/Billing Mismatch Filter

What does the filter do?

This filter screens for differences between the shipping information and the billing information (street, state, ZIP code, and country).

The specified action is taken whenever the shipping information differs from the billing information.

Data Normalization

The Shipping/Billing Mismatch filter is tolerant of minor address inaccuracies that result from typographical or spelling errors. The filter checks relationships among the street address, city, state, and ZIP code and determines if a minor change is needed before screening the transaction.

NOTE: This normalization is performed purely on the billing and shipping data, and does not authenticate the customer.

Because this normalization happens during data validation by the Payflow server, the data as entered by the customer will still appear in its original form on all transaction data review pages. This means that you might see the following entries not flagged as mismatches on the *Fraud Details* page:

Billing	**Shipping**
Steve Morrison	Steve Morrison
4390 Ramire***z***	4390 Ramire***s***
San Francisco, CA	San Fran***ci***sco, CA
9411***4***	9411***3***

How does the filter protect me?

There are legitimate reasons for a shipping/billing mismatch with a customer purchase—for example, gift purchases might fit this profile. But a mismatch could also indicate that someone

is using a stolen identity to complete a purchase (and having the items sent to another address from which they can retrieve the stolen items).

To help to distinguish between legitimate and fraudulent orders, review all mismatches by cross-checking other purchase information such as **AVS** and **card security code**.

Product Watch List Filter

What does the filter do?

The Product Watch List filter compares the SKUs (or other product identifier) of the products in a transaction against a Product Watch List that you create. Any transaction containing an SKU in the list triggers the filter. If you enable this filter, then you must set up the list of products that should be monitored.

NOTE: Items that you enter in the test Product Watch List are not carried over to the configuration for the live servers, so do not spend time entering a complete list for the test configuration.

How does the filter protect me?

Some products are attractive to fraudsters (especially popular products with high resale value like computers or televisions). The Product Watch List filter gives you the opportunity to review transactions involving such products to ensure that the order is legitimate.

High-risk Payment Filters

High-risk Payment Filters identify transactions that show billing/shipping discrepancies or an indication that someone other than the legitimate account holder is initiating the transaction.

AVS Failure Filter

What does the filter do?

This filter compares the street number and the ZIP code submitted by the customer against the data on file with the issuer.

The AVS response is composed of a **Y**, **N**, or **X** value for the customer's street address and a **Y**, **N**, or **X** value for the ZIP code. For example, the response for a correct street number and an incorrect ZIP code is **YN**.

If AVS information is not submitted with the transaction, then the response is **NN**.

TABLE A.1 AVS responses

Result	Meaning
Y	The submitted information matches information on file with the account holder's bank.
N	The submitted information does not match information on file with the account holder's bank.
X	The account holder's bank does not support AVS checking for this information.
(Null)	In some cases banks return no value at all.

AVS checks only for a street number match, not a street name match, so **123 Main Street** returns the same response as **123 Elm Street**. The "USPS Address Validation Failure Filter" on page 87 validates the address information

NOTE: .

The specified action is taken whenever the AVS response does not meet the criterion that you specified.

IMPORTANT: *The AVS Failure filter performs the action after the transaction is processed. This means that, if set to reject, the filter rejects the transaction after the transaction is authorized by the processor. To charge the customer for such a transaction, you must resubmit the transaction data.*

Specifying the Level of AVS Checking

Specify one of the AVS settings:

- **Full:** Take action if a transaction returns any value other than YY (Y for street address and Y for ZIP code).
- **Medi**um: Take action if a transaction returns values other than these: XX, XY, YX, and YY.
- **Light:** Take action only if NN is returned.

This table summarizes AVS levels:

TABLE A.2 AVS responses

AVS Setting	Allowed Responses
Full	(Y, Y)
Medium	(X, X), (X, Y), (Y, X), (Y, Y)
Light	(X, X), (X, Y), (Y, X), (X, N), (N, X), (N, Y), (Y, N), (Y, Y)

How does the filter protect me?

Buyers who can provide the street number and ZIP code on file with the issuing bank are more likely to be the actual account holder.

AVS matches, however, are not a guarantee. Use **card security code** and **Buyer Authentication** in addition to **AVS** to increase your certainty.

Card Security Code Failure Filter

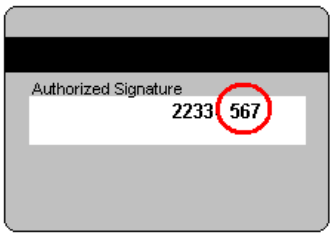
What does the filter do?

The card security code is a 3- or 4-digit number (not part of the credit card number) that appears on credit card. Because the card security code appears only on the card and not on receipts or statements, the card security code provides some assurance that the physical card is in the possession of the buyer.

IMPORTANT: *The Card Security Code Failure filter performs the action after the transaction is processed. This means that, if set to reject, the filter rejects the transaction after the transaction is authorized by the processor. To charge the customer for such a transaction, you must resubmit the transaction data.*

About the Card Security Code

The card security code is printed on the back of most cards (usually in the signature field). All or part of the card number appears before the card security code (**567** in the example). For American Express, the 4-digit number (**1122** in the example) is printed on the front of the card, above and to the right of the embossed account number. Be sure to explain this to your customers.



The card security code check compares the number provided by the customer with the number on file with the issuer and returns one of the following responses:

TABLE A.3 Card security code responses

Result	Meaning
Y	The submitted information matches information on file with account holder's bank.
N	The submitted information does not match information on file with the account holder's bank.

TABLE A.3 Card security code responses

Result	Meaning
X	Account holder's bank does not support this service.
(Null)	In some cases banks return no value at all.

Card Security Code Failure Filter Action

The specified action is taken whenever the card security code response is the value that you specified.

The Best Practices action is to review all transactions with responses other than **Y**. You set the "strength" of the filter as follows:

- **Full:** Take action if a value of **N** or **X** is returned.
- **Medium:** Take action only if a value of **N** is returned.

Buyer Authentication Failure Filter

You must enroll for the Buyer Authentication Service in the Fraud Protection Services suite to make use of the **Buyer Authentication Failure** filter. The filter is grayed out on configuration pages if you are not enrolled.

Buyer Authentication refers to the card-sponsored authentication services such as **Verified by Visa** and **MasterCard Secure Code** that make use of the 3-D Secure protocol. These authentication methods prompt buyers to provide a password to their card issuer before being allowed to execute a credit card purchase. The Buyer Authentication Service is described in "Buyer Authentication Service" on page 10.

What does the filter do?

The filter is triggered when the customer's identity is not adequately authenticated, according to criteria that you specify.

Buyer Authentication Results

Although MasterCard and Visa both use the underlying 3-D Secure protocol to implement the Buyer Authentication service, they have different liability rules regarding buyer authentication results. Those rules appear in Table A.4.

MasterCard converts 3-D Secure results into UCAF fields. To simplify for the merchant, all responses are normalized into the values listed in Table A.4.

Buyer Authentication returns one of the following responses in the `AUTHENTICATION_STATUS` name-value pair (values are for Visa USA region):

TABLE A.4 Responses in the AUTHENTICATION_STATUS name-value pair

Result	Description	Liability Impact (Subject to Change)
Y	Successful authentication—the password was correct.	Both Visa and MasterCard shift liability for fraud from the merchant.
A	The merchant attempted to authenticate the buyer, but the issuer does not support buyer authentication.	Visa shifts liability for fraud from the merchant. MasterCard does not shift liability for fraud from the merchant.
N	Unsuccessful authentication—the password was not correct.	Neither Visa nor MasterCard shift liability for fraud from the merchant.
U	Authentication could not be completed due to network error.	Neither Visa nor MasterCard shift liability for fraud from the merchant.
F	Card issuers authentication credentials could not be validated.	Neither Visa nor MasterCard shift liability for fraud from the merchant

Actions

You set the "strength" of the filter as follows:

- **Full:** Trigger if a value of **N**, **U**, or **F** is returned.
- **Medium:** Trigger only if a value of **N** is returned.

NOTE: To enforce the minimum Visa regulations, set the filter to **Medium** strength with an action of **Reject**. This setting rejects **N** responses, however, so there is no liability benefit.

How does the filter protect me?

Buyer Authentication is the only screening tool that promises to shift fraud liability from the merchant. The password used with **Verified by Visa** and **MasterCard Secure Code** is the digital equivalent to a shopper's handwritten signature.

NOTE: Make use of **Buyer Authentication** if your processor and acquirer support it. The use of the password protects merchants from some chargebacks when a customer claims not to have authorized the purchase.

Widespread account holder enrollment in Buyer Authentication programs may take some time and depends on the card issuers supporting and marketing the option.

BIN Risk List Match Filter

What does the filter do?

The Bank Identification Number (BIN) makes up the first six digits of a credit card number. The BIN identifies the bank that issued the card. This filter screens every credit card number for BINs on the high-risk list.

The specified action is taken whenever a BIN matches one on the list.

How does the filter protect me?

Certain BINs might be associated with a greater degree of fraud because the issuer uses less stringent authentication policies when issuing cards. In other cases, because some issuers have a large number of cards in circulation, the cards are more likely to fall into the hands of fraudsters.

Account Number Velocity Filter

What does the filter do?

The Account Number Velocity filter triggers when any credit card account number is used five times within a three-day (72-hour) period.

IMPORTANT: *The specified action is performed on only the transaction that triggered the filter and not on the previous four transactions. You must manually review and act upon those transactions. Generate a Transaction Details report and click the Account Velocity link to view the transactions.*

What is Velocity?

In the risk management industry, an event's *velocity* is a measure of its frequency of occurrence during a defined time period. Unusually high velocity is can be associated with a fraudster making repeated attacks on a system. Legitimate customers do not typically perform multiple transactions in quick succession.

How does the filter protect me?

Fraudsters often submit multiple purchases with a single account number to try to discover the card's valid billing address or card security code. Alternatively, the fraudster may attempt to bypass ceiling filters by making multiple small purchases with a know good account number.

High-risk Address Filters

High Risk Address Filters identify transactions associated with high-risk geographical locations or poorly-matched transaction data.

ZIP Risk List Match Filter

What does the filter do?

This filter compares the **Ship To** and **Bill To** ZIP codes (US only) against the high-risk list. High-risk ZIP codes are determined based on analysis of millions of e-commerce transactions.

The specified action is taken whenever a submitted ZIP code appears in the risk list.

NOTE: Fraud tends to correlate to densely populated areas like major cities. For this reason, ZIP codes on the risk list will likely correlate to major cities.

How does the filter protect me?

Matching a ZIP code on the risk list does not necessarily indicate a fraudulent purchase, but that you should evaluate these transactions more closely than other transactions.

Freight Forwarder Risk List Match Filter

What does the filter do?

This filter screens the full **Ship To** address against a list of addresses of freight forwarders.

NOTE: Unlike the other Risk Lists, the Freight Forwarder Risk List was not developed through statistical evaluation of e-commerce transactions. Rather, this is a list of know addresses associated with freight forwarders.

The specified action is taken whenever a shipping address matches the address of a known freight forwarding service.

NOTE: The **Freight Forwarder** filter requires a valid US shipping address. If the **USPS Address Validation** filter determines that the address does not exist, then the **Freight Forwarder** filter is skipped and placed in the **Unused Filters** list on the *Fraud Details* page.

How does the filter protect me?

Freight forwarding services enable a customer to open an account using the forwarder's corporate address, and to have the service forward all packages to another end destination. While there are legitimate uses for a freight forwarding service, forwarders also enable fraudsters to hide their true location.

Whenever a customer orders delivery to a freight forwarder, you should research the transaction more closely.

USPS Address Validation Failure Filter

What does the filter do?

This filter screens the **Ship To** and **Bill To** addresses (street number, street name, state, and ZIP code) against the United States Postal Service database of existing addresses. The USPS updates the database continually.

The specified action is taken whenever the address cannot be validated (it does not exist or is incorrect in some way).

NOTE: The filter does not validate that the person named in the transaction data lives at that address or even that the address is currently occupied—only that the address exists in the database.

How does the filter protect me?

To trick a merchant's filters, fraudsters sometimes deliberately misspell or make up street names. This enables the fraudster to spoof AVS, geo-location, and high-risk address filters. You can identify this basic form of spoofing by using the USPS Address Validation filter to determine whether an address really exists.

NOTE: One useful side effect of the filter is that mis-keyed addresses of legitimate customers can be identified before shipping.

IP Address Match Filter

What does the filter do?

This filter screens the IP address from which a transaction originates against a list of high-risk IP addresses. An IP (Internet protocol) address is a unique identifier for a computer on a TCP/IP network that can identify a particular network and a particular computer on that network.

NOTE: IP Addresses are not always fixed like the addresses to physical buildings. Some computers get a new IP address each time they connect to a network. The most general level of the IP address indicates the region or country from which the computer is connecting, and is thus relatively fixed. Therefore the IP Address risk list is most effective as a screen for overseas fraud.

The specified action is taken whenever a submitted IP address appears in the risk list.

How does the filter protect me?

A customer's IP address identifies a country, region, state, or city. As with ZIP codes, these addresses can be associated with higher or lower likelihood of fraud. This is especially true with high-risk countries that are known to be associated with especially high rates of fraud.

Required Transaction Data

You must send the customer's IP address to use this filter.

Email Service Provider Risk List Match Filter

What does the filter do?

This filter compares the e-mail service provider used by the customer against a list of high-risk e-mail service providers.

NOTE: Fraudsters most often use free services at which they do not need to provide traceable billing information. (Free services are also popular among legitimate shoppers—because they are free.)

It is therefore a good practice to check whether the billing name appears in some form in the e-mail address. For example, Tina Johnson should have an e-mail address of TinaJohnson@hotmail.com or Johnson42@hotmail.com, or some similar variant. Such an e-mail address is less suspicious than xy12@hotmail.com.

The specified action is taken whenever the e-mail service provider is found in the risk list.

How does the filter protect me?

Online merchants rarely talk to their customers. The customer's e-mail address is a critical communications channel between the merchant and customer. For example, e-mail is often used to confirm a purchase and to notify the customer that shipment has been made.

It is therefore important for merchants to determine how reliably the e-mail address is tied to the identity of the customer. Some e-mail service providers make it especially easy to open and close e-mail accounts without ever providing personal information, enabling fraudsters to use false identities to cover their tracks.

You should examine any transaction in which a high-risk e-mail service provider is involved.

Geo-location Failure Filter

What does the filter do?

This filter compares the IP address of the customer's computer (captured in real-time when the transaction is submitted) and compares its geographical location to the billing and shipping addresses. IP (Internet protocol) addresses are unique identifiers for computers that can often be mapped to a specific city or area code.

The specified action is taken whenever the IP address, shipping address, and billing address do not fall within a 100 mile radius. If you provide only one physical address (billing or shipping address), then the filter triggers when the distance between the IP address and the address that you provided is greater than 100 miles.

NOTE: Gift purchases shipped far from the billing address will trigger the filter.

Every effort has been made to ensure that IP address mapping is accurate and up-to-date. Given the nature of the Internet's architecture, however, some Internet Service Providers use data centers far from the customers being serviced. In addition, as described in the **IP Address Risk List Match** filter, IP addresses can change dynamically. For these reasons, treat this filter as an indicator of suspicious activity, not as a definitive result.

How does the filter protect me?

Comparing the geographical location associated with the IP address to the submitted shipping and billing information can be an effective method for identifying identity spoofing. Fraudsters often pretend to live in a location, but live and shop from another.

All three elements should match one realistic customer profile. For example, a customer with a billing address in New York would typically shop from a computer in New York, and request delivery to a New York address. While there may be some minor inconsistencies in the overall profile, it should generally fit together. Remember, however, that gift purchases sent to another part of the country will not fit this profile.

NOTE: You should be especially wary when a customer has an international IP address but uses U.S. billing and shipping information.

IP Address Velocity Filter

What does the filter do?

The IP Address Velocity filter triggers when five or more transactions within three days (72 hours) originate from any individual IP address.

IMPORTANT: *The specified action is performed on only the transaction that triggered the filter and not on the previous four transactions. You must manually review and act upon those transactions. Generate a Transaction Details report and click the IP Address Velocity link to view the transactions.*

IP addresses do not always identify a unique computer or user. For example, an Internet Service Provider (ISP) may use a limited number of IP addresses for all of its users. To protect against triggering the filter in this case, set up an IP Address Velocity Ignore List (described in the online help).

What is Velocity?

In the risk management industry, an event's *velocity* is a measure of its frequency of occurrence during a defined time period. Unusually high velocity is can be associated with a fraudster making repeated attacks on a system. Legitimate customers do not typically perform multiple transactions in quick succession.

How does the filter protect me?

Fraudsters often submit multiple purchases using an automated script that tests unknown card numbers. Alternatively, the fraudster may attempt to bypass other filters by making multiple small purchases with multiple stolen account numbers.

High-risk Customer Filters

Bad Lists

What does the filter do?

This filter compares the customer's e-mail address and credit card number against lists (that *you* create) of addresses and numbers for known bad customers.

NOTE: Unlike the Risk lists managed by PayPal, you, solely, manage and update the Bad Lists.

Any transaction that is an exact match with an entry in one of your bad lists triggers the filter.

If you enable this filter, then your next step will be to set up lists of bad email addresses and bad card numbers. Be sure to type the e-mail addresses and credit card numbers accurately. Enter only numerals in the credit card number list—no spaces or dashes.

NOTE: Items that you enter in the test **Bad** lists are not carried over to your configuration for the live servers, so do not spend time entering a complete list for the test configuration.

How does the filter protect me?

This filter enables you to block repeat fraud.

In the e-commerce world, once someone successfully performs a fraudulent transaction, they are very likely to try again. For this reason, you should set up lists of cards and email addresses and configure this filter to take action on transactions with data elements appearing in the bad lists.

International Order Filters

International Order Filters identify transactions associated with risky international locations.

Country Risk List Match Filter

What does the filter do?

This filter screens the customer's shipping and billing address information for matches with countries on the list of high-risk countries.

The specified action is taken whenever any of the information matches a country on the risk list.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens and the difficulty of cross-border legal enforcement against fraudulent activities.

Certain countries, however, are much riskier than others. These countries have high likelihood of fraud and you should evaluate transactions from these countries closely.

International Shipping/Billing Address Filter

What does the filter do?

This filter screens the customer's shipping and billing information for non-U.S. addresses. The filter checks for country code 840, or any derivation of "United States" (U.S., USA, United

States of America, America, and so on) in the country fields. Any other country name triggers the filter.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens and the difficulty of cross-border legal enforcement against fraudulent activities.

The **International Shipping/Billing Address** filter sets aside transactions from customers in foreign countries so that you can evaluate them more fully.

International IP Address Filter

What does the filter do?

This filter screens for international IP addresses. An IP (Internet protocol) address is a unique identifier for a computer that can identify a particular network and a particular computer on that network.

The specified action is taken whenever the IP address indicates an international computer or network.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens as well as the difficulty of cross-border legal enforcement against fraudulent activities.

The **International IP Address** filter sets aside transactions from customers in foreign countries so that you can evaluate them more fully.

International AVS Filter

What does the filter do?

International Address Verification Service (IAVS), determines whether the issuer is domestic (US) or international.

TABLE A.5 AVS filter results

Result	Meaning
Y	The card number is associated with an international issuer.
N	The card number is associated with a US issuer.
X	Account holder's bank does not support IAVS.
(Null)	In some cases banks return no value at all.

The specified action is taken whenever AVS returns **Y**.

Special Requirements

- You must use Payflow Pro client version 3.06 or newer to use the IAVS filter.
- International AVS is not currently widely supported by processors. Check to see if your processor supports international AVS.
  - FDMS Nashville and NOVA return IAVS responses for all card types.
  - EDS Aurora and FDMS South return IAVS responses for VISA cards only.
  - All other processors always return **N** or **X**.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens as well as the difficulty of cross-border legal enforcement against fraudulent activities.

The **International AVS** filter sets aside transactions from customers with cards issued in foreign countries so that you can evaluate them more fully.

Accept Filters

Accept Filters immediately approve transactions that meet characteristics that you specify. If a filter in this group is triggered, then the transaction is accepted regardless of Review filter results.

IMPORTANT: *The Accept filters are designed to reduce the load on your staff by reducing the number of transactions set aside for review. The Accept filters do not reduce risk.*

Good Lists

What does the filter do?

This filter compares the customer's e-mail address and credit card number against lists (that *you* create) of addresses and numbers for known good customers. *You* create the lists.

Any transaction for which the e-mail address or credit card number is an exact match with an entry in one of your good lists is accepted and no other filters are applied. Enter only numerals in the credit card number list—no spaces or dashes.

NOTE: Unlike the Risk lists that PayPal manages, you, solely, manage and update the Good Lists.

Items that you enter in the test Good lists are not carried over to your configuration for the live servers, so do not spend time entering a complete list for the test configuration.

If you activate this filter, then you must set up lists of good email addresses and good card numbers. Be sure to type the e-mail addresses and credit card numbers accurately.

IMPORTANT: *The Good Lists do not authenticate individuals. If a fraudster were to steal e-mail addresses or credit card account numbers from this list, then they would be able to bypass the filter.*

How does the filter protect me?

To ensure that loyal repeat customers are not held up by your fraud review process, you may want to create lists of e-mail addresses and card numbers that should be accepted. This ensures that an abnormal shopping pattern on the part of a loyal customer (for example making a purchase while on vacation overseas) does not trigger a filter and delay the transaction.

Total Purchase Price Floor Filter

What does the filter do?

This filter screens the total amount of a transaction (including tax, shipping and handling fees).

If a transaction amount is below the price set for this filter, then the transaction is accepted and no other filters are applied.

How does the filter protect me?

Merchants with an especially high transaction volume can use this filter to reduce the number of transactions that their staff must review—transactions below the specified price level are accepted *without further analysis*.

Custom Filters

You create Custom filters by combining up to five existing filters. A well-designed Custom filter can more accurately identify suspicious transactions because it is fine-tuned to the unique needs of your business (for example, you can specify a particular combination of amount, buyer location, and shipping location). For this reason, fewer legitimate transactions are unnecessarily held for review.

For example, a Custom filter that triggers only when both the Card Security Code Failure and AVS Failure filters trigger will set aside transactions that are quite suspicious.

NOTE: You can create a combined maximum (test plus live) of 15 Custom Filters. For example, if you currently have 5 test Custom Filters and 10 live Custom Filters, you cannot create any more Custom Filters until you delete one of the existing Custom Filters.

See PayPal Manager online help for details on creating a custom filter.

B Testing the Transaction Security Filters

Each example transaction shown in this chapter is designed to test the operation of a single filter. To test a filter, disable all other filters and submit the transaction. The filter should be triggered and display its results in the *Transaction Details* page.

In the examples, the critical transaction data is shown in **bold red** type.

In This Appendix

- "Good and Bad Lists" on page 95
- "AVS Failure Filter" on page 96
- "BIN Risk List Match Filter" on page 96
- "Country Risk List Match Filter" on page 91
- "Email Service Provider Risk List Match Filter" on page 98
- "Freight Forwarder Risk List Match Filter" on page 98
- "Geo-location Failure Filter" on page 99
- "International AVS Filter" on page 99
- "International IP Address Filter" on page 100
- "International Shipping/Billing Address Filter" on page 101
- "IP Address Match Filter" on page 102
- "Shipping/Billing Mismatch Filter" on page 102
- "Total Item Ceiling Filter" on page 103
- "Total Purchase Price Ceiling Filter" on page 103
- "Total Purchase Price Floor Filter" on page 104
- "USPS Address Validation Failure Filter" on page 104
- "ZIP Risk List Match Filter" on page 105

Good and Bad Lists

To test the Good and Bad List filters, add good and bad entries to the list and then submit a transaction using a value in the list.

AVS Failure Filter

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[4]=1.02&BILLTOPHONE2=650-555-
0123&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COMMENT1=Automated testing
from
AdminTester&COUNTRY=US&CUSTIP=194.213.32.220&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DO
B=CA123456&EMAIL[17]=Admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&L
ASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&
L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Mountain
View&COUNTRYCODE=US&SHIPTOEMAIL[17]=Admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAM
E&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-
555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield
Road&SHIPTOSTREET2=487 East Middlefield
Road&SHIPTOZIP=94043&SS=565796510&STATE=CA&STREET=667 W. Rincon
Ave&BILLTOSTREET2=Unit
C&TAXAMT=1.02&TENDER=C&USER=TESTAVSRejectFull&VENDOR=TESTAVSRejectFull&ZIP=99999"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VBCA25034255&RESPMSG=Declined by Fraud
Service&AUTHCODE=421PNI&AVSADDR=X&AVSZIP=X&IAVS=X&PREFPSMSG=No Rules
Triggered&POSTFPSMSG=Reject AVS
    !!ERROR 16:55:6 result=125 TRXTYPE=A!!
```

BIN Risk List Match Filter

Pass in the appropriate credit card number for the card brand:

- American Express: 378282246310005
- MasterCard: 5555555555554444
- Visa: 4610251000010168

```
 "TRXTYPE=A&ACCT=4610251000010168&AMT[8]=$1000.00&BILLTOPHONE2=650-555-
0123&BILLTOSTREET2=123 BILLTOSTREET&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11,
2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No City&COMMENT1=Automated
testing from
AdminTester&COUNTRY=203&CUSTIP=66.218.71.93&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB
=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LA
STNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L
_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&COUNTRYCODE=203&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNA
ME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-
555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskBinCheckReject&VENDOR=TESTHighRiskBinCheckRej
ect&ZIP=11111"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25033363&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskBinCheck
    !!ERROR 15:52:54 result=125 TRXTYPE=A!!
```

Country Risk List Match Filter

Pass in the specified country or country code.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=AD&COUNTRYCODE=AD&CUSTIP=172.131.193.25&CUSTREF=CUSTREF&DESC=DESC
&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FR
EIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L
_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650
-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskCountryCheckReject&VENDOR=TESTHighRiskCountry
CheckReject&ZIP=60649"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25031715&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskCountryCheck
    !!ERROR 14:7:57 result=125 TRXTYPE=A!!
```

Email Service Provider Risk List Match Filter

Pass in the specified e-mail address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=AD&COUNTRYCODE=AD&CUSTIP=172.131.193.25&CUSTREF=CUSTREF&DESC=DESC
&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FR
EIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L
_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650
-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskEmailCheckReject&VENDOR=TESTHighRiskEmailChec
kReject&ZIP=60649"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25031907&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskEmailCheck
    !!ERROR 14:20:5 result=125 TRXTYPE=A!!
```

Freight Forwarder Risk List Match Filter

Pass in the specified shipping address.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[5]=$1000&BILLTOPHONE2=650-555-
0123&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Indianapolis&COMMENT1=Automated
testing from
AdminTester&COUNTRY=US&CUSTIP=255.255.255.255&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&D
OB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&
LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0
&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Indianapolis&COUNTRYCODE=US&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIP
TOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHO
NE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=IN&SHIPTOSTREET=973 N Shadeland
Ave&SHIPTOSTREET2=UNIT #C&SHIPTOZIP=46219&SS=565796510&STATE=IN&STREET=973 N
Shadeland&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskFreightCheckReject&VENDOR=TESTHighRis
kFreightCheckReject&ZIP=46219"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25087954&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskFreightCheck
    !!ERROR 15:43:53 result=125 TRXTYPE=A!!
```

Geo-location Failure Filter

Pass in the specified Shipping address, billing address, and IP address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BILLTOPHONE2=650-555-
0123&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COMMENT1=Automated testing
from
AdminTester&COUNTRY=US&CUSTIP=192.6.165.40&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=
CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LAS
TNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_
UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Mountain
View&COUNTRYCODE=US&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAM
E&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-
555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield
Road&SHIPTOSTREET2=487 East Middlefield
Road&SHIPTOZIP=94043&SS=565796510&STATE=CA&STREET=236 W. Rincon
Ave&BILLTOSTREET2=Unit
C&TAXAMT=1.01&TENDER=C&USER=TESTGeoLocationCheckReject&VENDOR=TESTGeoLocationCheckRej
ect&ZIP=95008"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25088015&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject GeoLocationCheck
    !!ERROR 15:44:28 result=125 TRXTYPE=A!!
```

International AVS Filter

Pass in the specified ZIP codes and billing address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=US&COUNTRYCODE=USA&CUSTIP=66.218.71.93&CUSTREF=CUSTREF&DESC=DESC&
DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FRE
IGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_
TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-
555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=00101&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTInternationalAVSReject&VENDOR=TESTInternationalAVSRej
ect&ZIP=00101"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VBCA25032988&RESPMSG=Declined by Fraud
Service&AUTHCODE=890PNI&AVSADDR=Y&AVSZIP=Y&IAVS=Y&PREFPSMSG=No Rules
Triggered&POSTFPSMSG=Reject InternationalAVS
    !!ERROR 15:30:41 result=125 TRXTYPE=A!!
```

International IP Address Filter

Pass in the specified IP address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COMMENT1=Automated testing
from
AdminTester&COUNTRY=US&COUNTRYCODE=US&CUSTIP=194.213.32.220&CUSTREF=CUSTREF&DESC=DESC
&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FR
EIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L
_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650
-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Mountain
View&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield
Road&SHIPTOSTREET2=487 East Middlefield
Road&SHIPTOZIP=94043&SS=565796510&STATE=CA&STREET=236 W. Rincon
Ave&BILLTOSTREET2=Unit
C&TAXAMT=1.01&TENDER=C&USER=TESTNonUSIPAddressReject&VENDOR=TESTNonUSIPAddressReject&
ZIP=95008"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25032282&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject NonUSIPAddress
    !!ERROR 14:49:23 result=125 TRXTYPE=A!!
```

International Shipping/Billing Address Filter

Pass in a non-US Country code to either the billing or shipping address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=CZ&COUNTRYCODE=USA&CUSTIP=66.218.71.93&CUSTREF=CUSTREF&DESC=DESC&
DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FRE
IGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_
TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-
555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTInternationalOrderReject&VENDOR=TESTInternationalOrde
rReject&ZIP=11111"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25032493&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject InternationalOrder
    !!ERROR 15:0:24 result=125 TRXTYPE=A!!
```

IP Address Match Filter

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[6]=$75.00&BILLTOPHONE2=650-555-
1234&BILLTOSTREET2=&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No City&COMMENT1=Test to trigger
rules&COUNTRY=US&CUSTIP=172.131.193.25&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA12
3456&EMAIL[21]=lastName@paypal.com&EXPDATE=1209&FIRSTNAME=FirstName&FREIGHTAMT=1.11&L
ASTNAME=LastName&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0
&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-
1234&PONUM=PONUM&PWD=password1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCI
TY=No
City&COUNTRYCODE=US&SHIPTOEMAIL[17]=test@paypal.com&SHIPTOFIRSTNAME=&SHIPTOLASTNAME=&
SHIPTOMIDDLENAME=&SHIPTOPHONE=650-555-1235&SHIPTOPHONE2=650-555-
1236&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield
Road&SHIPTOSTREET2=&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=487 East northfield
Road&BILLTOSTREET2=&TAXAMT=1.01&TENDER=C&USER=testFilters&VENDOR=TESTFilters&ZIP=1507
1"
```

Shipping/Billing Mismatch Filter

Pass in the specified shipping and billing addresses.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=J
uly 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=255.255.255.255&CUSTREF=CUSTREF&DESC=D
ESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John
&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU
0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=
650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPT
OLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-
0125&SHIPTOSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123 SHIPTOSTREET
2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main
St.&TAXAMT=1.01&TENDER=C&USER=TESTBillShipMismatchReject&VENDOR=TESTBillShipMismatchR
eject&ZIP=11111"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25031150&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject BillShipMismatch
    !!ERROR 13:34:27 result=125 TRXTYPE=A!!
```

Total Item Ceiling Filter

First, set the filter to trigger on 5 or fewer items. For testing, pass in more than 5 items, as shown here.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=J
uly 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=255.255.255.255&CUSTREF=CUSTREF&DESC=D
ESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John
&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=6&L_SKU0=L_SKU
0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=
650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPT
OLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-
0125&SHIPTOSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123 SHIPTOSTREET
2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main
St.&TAXAMT=1.01&TENDER=C&USER=TESTHighOrderNumberReject&VENDOR=TESTHighOrderNumberRej
ect&ZIP=11111"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25030952&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighOrderNumber
    !!ERROR 13:19:25 result=125 TRXTYPE=A!!
```

Total Purchase Price Ceiling Filter

First, set the filter to trigger at 1000.00. For testing, pass in an amount higher than 1000, as shown here.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[7]=1000.01&BROWSERCOUNTRYCODE=203&BROWSERTIME[22
]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=255.255.255.255&CUSTREF=CUSTREF&DESC=D
ESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John
&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU
0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=
650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPT
OLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-
0125&SHIPTOSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123 SHIPTOSTREET
2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main
St.&TAXAMT=1.01&TENDER=C&USER=TESTCeilingAmountReject&VENDOR=TESTCeilingAmountReject&
ZIP=11111"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25030756&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject CeilingAmount
    !!ERROR 13:11:4 result=125 TRXTYPE=A!!
```

Total Purchase Price Floor Filter

To test the Total Purchase Price Floor filter, submit a transaction with an amount lower than the trigger amount.

USPS Address Validation Failure Filter

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=US&COUNTRYCODE=US&CUSTIP=203.81.64.19&CUSTREF=CUSTREF&DESC=DESC&D
L=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FREI
GHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_T
YPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-
555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&COUNTRYCODE=US&SHIPTOSTREET=123 Main
St. blah&SHIPTOSTREET2=&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123 Main St.
blah&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTBillUSPostalAddressCheckReject&VENDOR=TESTBillUSPosta
lAddressCheckReject&ZIP=60649"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25032101&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject BillUSPostalAddressCheck
    !!ERROR 14:39:3 result=125 TRXTYPE=A!!
```

ZIP Risk List Match Filter

Pass in the specified ZIP codes.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSERCOUNTRYCODE=203&BROWSERTIME[2
2]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=172.131.193.25&CUSTREF=CUSTREF&DESC=DE
SC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&
FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0
&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=6
50-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main
St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123
Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskZIPCheckReject&VENDOR=TESTHighRiskZIPCheckRej
ect&ZIP=60649"
```

Expected Response Message

```
resp mesg=RESULT=125&PNREF=VB0A25031523&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskZIPCheck
    !!ERROR 13:55:6 result=125 TRXTYPE=A!!
```

C Testing Buyer Authentication Transactions Using the Payflow SDK

This chapter describes the process of testing Buyer Authentication transactions using the Payflow SDK. For complete information on using the SDK, see *Payflow Pro Developer's Guide*.

The content and format of responses to transaction requests are described in "Buyer Authentication Transaction Parameters and Return Values" on page 40.

In This Appendix

- "Testing Buyer Authentication Transactions" on page 107
- "Test Case Descriptions and Account Numbers" on page 107
- "Expected Result Codes for Buyer Authentication" on page 109
- "Buyer Authentication Testing Procedures" on page 110

Testing Buyer Authentication Transactions

Test cases are described in "Test Case Descriptions and Account Numbers" on page 107. Use the card number associated with a test case and the appropriate password to generate the results appropriate to the case.

Buyer Authentication Test Server

Direct **Verify Enrollment** transactions (TRXTYPE=E) and **Validate Authentication** transactions (TRXTYPE=Z) to the test Buyer Authentication Server:

pilot-buyerauth.verisign.com

Payflow Test Server

Direct the standard Payflow sale or authentication test transaction to:

pilot-payflowpro.paypal.com

Test Case Descriptions and Account Numbers

To generate particular results, use the test account numbers listed in Table C.1.

Account numbers starting with 5 are MasterCard. Numbers starting with 4 are Visa. In the table, VE stands for the Verify Enrollment transaction and VA stands for the Validate Authentication transaction.

Test Cases

TABLE C.1 Generating buyer authentication result

Case	Test Scenario	Test Account Number
1	Card enrolled (VE AUTH_STATUS=E) Successful authentication (AUTH_STATUS=Y for VA) Successful signature verification	5100000000000008 5200000000000007 4000000000000002 4000000000000101
2	Card enrolled (VE AUTH_STATUS=E) Failed authentication (AUTH_STATUS=N for VA) Successful signature verification	5100000000000008 5200000000000007 4000000000000002 4000000000000101
3	Card enrolled (VE AUTH_STATUS=E) Attempt authentication (VA AUTH_STATUS=A) Successful signature verification	4111111111111111
4	Card not enrolled (VE AUTH_STATUS=O)	5105105105105100 4000000000000507
5	Can not verify card enrollment (VE AUTH_STATUS=X)	5555555555554444 4012888888881881
6	Card eligible for authentication (VE AUTH_STATUS=E) User cancelled authentication by clicking the Cancel button on the ACS page.	5100000000000008 5200000000000007 4000000000000002 4000000000000101
7	Card enrolled for authentication (VE AUTH_STATUS=E) Unable to authenticate (VA AUTH_STATUS=U) Successful signature verification	5300000000000006 4000000000000309
8	Card enrolled (VE AUTH_STATUS=E) VA transaction error (VA AUTH_STATUS=F)	5500000000000004
12	Merchant not registered for this feature or is deactivated. (merchant authentication failure)	Any valid MasterCard or Visa account number

Expected Result Codes for Buyer Authentication

IMPORTANT: *All returned name-value pairs for transactions with the Buyer Authentication Server include length tags. Length tags specify the exact number of characters and spaces that appear in the value. For example, RESPMSG[2]=OK.*

The following Result Codes (RESULT return values) are associated with the Buyer Authentication Service. The full list of Result Codes appears in "RESULT Codes and RESPMSG Values" on page 68.

TABLE C.2 Buyer Authentication Service Result codes

Result Code	Description
0	Successful
3	Invalid transaction type
4	Invalid amount
7	Field format error
23	Invalid or missing account number
24	Invalid or missing expiration date
1001	Service unavailable
1002	Transaction timeout
1003	Invalid client version
1004	Invalid timeout value
101	Service unavailable
1012	Service unavailable
1013	Service unavailable
1014	Merchant has not activated buyer authentication for this card type
1021	Invalid card type
1022	Invalid or missing currency code
1023	Merchant has not activated buyer authentication for this card type
1041	Validate Authentication failed: missing or invalid PARES
1042	Validate Authentication failed: PARES format is invalid
1043	Validate Authentication failed: Cannot find successful Verify Enrollment
1044	Validate Authentication failed: Signature validation failed for PARES

TABLE C.2 Buyer Authentication Service Result codes

Result Code	Description
1045	Validate Authentication failed: Mismatched or invalid amount in PARES
1046	Validate Authentication failed: Mismatched or invalid acquirer in PARES
1047	Validate Authentication failed: Mismatched or invalid Merchant ID in PARES
1048	Validate Authentication failed: Mismatched or invalid card number in PARES
1049	Validate Authentication failed: Mismatched or invalid currency code in PARES
1050	Validate Authentication failed: Mismatched or invalid XID in PARES
1051	Validate Authentication failed: Mismatched or invalid order date in PARES
1052	Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction

Buyer Authentication Testing Procedures

Follow these steps to test your Buyer Authentication integration:

Perform the Verify Enrollment Transaction

Direct the **Verify Enrollment** transaction (TRXTYPE=E) to the test buyer authentication server: **pilot-buyerauth.verisign.com**

```
"TRXTYPE=E&ACCT=5105105105105100&AMT=19.25&EXPDATE=1203&PARTNER=PayPal&PWD=
p12345&VENDOR=SuperMerchant&USER=SuperMerchant"
```

Verify Enrollment Transaction Test Cases

TABLE C.3 Verify Enrollment test cases

AUTH_STATUS of Verify Enrollment Transaction	Test Case
E (Card Eligible for authentication)	1, 2, 3, 6, 7, 8
O (Attempt not available)	4
X (Unable to fulfill request)	5

Example Return Values

NOTE: AUTHENTICATION_ID, AUTHENTICATION_STATUS, and ECI should be returned in all cases. For buyer authentication transaction types, the AUTHENTICATION_ID value performs the same function as the PNREF value that is returned to standard Payflow transactions.

- **Account is enrolled in the 3-D Secure program**

  If the cardholder is enrolled (test cases 1, 2, 3, 6, 7, and 8), then the AUTHENTICATION_STATUS should be E, and PAREQ and ACSURL should return non-null values.

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=f43669e4921cf8b504c4&AUT
HENTICATION_STATUS[1]=E&PAREQ[428]=eJxVku1ugjAUhm+FeAH0A3Bozpr48WP+2GK23
UA9HJVECpYy9e7XCkzXkPS8fcvD6Vvg+2iJ1l+EnSUF79S2+kBRWbxO9mkync4onUmB+3yX8
RTTiYLt4pPOCn7ItmVtlIh5LIGN0hMsHrVxCjSel5sPJcMANiioyG7WSgwDWK/B6IrUkloXr
fTpVJqDn20Rreqq0eYG7O4D1p1x9qbylAMbBXT2pI7ONXPGLpdLvPMU7CHoGTHWFbCwB9iju
W0XqtYzr2Whpi+5FEWOlGOWU06U7f0HggOFdqQk5wmXIokEn3M5T1Jg93XQVWhCiVksM3/GX
kET4IvRCs7zCvioLRkcjzEqoGtTG/I7fFx/NRTUom99mB59r95CxOh8epngzw8Pad+NgLSKJ
6InWg8Ir7HhDtlw3b769xv8AhQarWM=&ACSURL[66]=http://pilot-buyerauth-
post.verisign.com/DDDSecure/Acs3DSecureSim/start
```

- **All other cases**

  If the cardholder is not enrolled or other conditions (test cases 4 and 5), then the following is returned:

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=48c92770755039d6bb3d&AUT
HENTICATION_STATUS[1]=O&ECI[1]=1
```

  PAREQ and ACSURL should not be returned, but AUTHENTICATION_ID and ECI must be returned. (for example, test case 4 with a test MasterCard account):

Step 1 POST the PAREQ to the ACS URL

PAREQ and ACSURL values are returned for test cases 1, 2, 3, 6, 7, and 8. For other cases, skip to "Submit the Payflow Sale or Authorization transaction with buyer authentication data" on page 115.

1. Construct an HTML page with a form that performs a POST to the ACS Simulator (http://pilot-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/start) The form must contain the following fields (fieldnames are case-sensitive):

   PAREQ — Copy and paste the PAREQ value from the previous step.

   TermUrl — The merchant URL to which the reply must be posted. For testing, use: https://pilot-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/pares

   MD — The Merchant Data field: Merchant state data that must be returned to the merchant. This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session. Since the content of this field varies by merchant implementation, the ACS must preserve it unchanged and without assumptions about its content.

   The MD field must contain only ASCII characters in the range 0x20 to 0x7E. If other data is needed, then the field must be Base64-encoded. The size of the field (after Base64 encoding, if applicable) is limited to 1024 bytes.

   If MD includes confidential data (such as the PAN), then it must be encrypted.

2. POST to the ACS Simulator.

   (http://pilot-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/start)

3. The results depend upon the test account number that you used:

   – For test cases 1, 2, 6, and 8, the ACS page appears and prompts for a password. The correct password (**password**) results in an authenticated user. Enter any other string to test case 2.
   – For test case 3 (attempted authentication of a card that is not enrolled—Visa only), ACS does not display a page asking for cardholder's password but directly generates a PAREQ and POSTs it back to the specified TermUrl.

Step 2 Validate Authentication Transaction

Validate Authentication Transaction Test Cases

TABLE C.4 Validate Authentication test cases

AUTHENTICATION_STATUS of Validate Authentication Transaction	Test Case
Y	1
N	2
A (Visa only)	3
U	7
F	8

Procedure

Direct the **Validate Authentication** transaction (TRXTYPE=Z) to the test buyer authentication server: **pilot-buyerauth.verisign.com**. Use the PARES value from the ACS return POST or use the example value that appears on page 114.

IMPORTANT: *To avoid format errors, the submitted* `PARES` *value should be a single line with no carriage returns (check especially at the end of the message).*

For this call, you must use the **pfpro_file.exe** script—do not use the **pfpro.exe** client. Save the **Validate Authentication** transaction in a file and then use the **pfpro_file** script to send the request to the test Buyer Authentication server:

Example Validate Authentication transaction

```
"TRXTYPE=Z&PARTNER=PAYPAL&PWD=p12345&VENDOR=SuperMerchant&USER=SuperMerchan
t&PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQUrWYU3NllEUUBAfv0kWl1l91TPX
ebhTowRBpmHkyfPfr5gbiRlFHF6FFzKaDFXoqry4uhTGn77PAvH4SQKp1MvmEbTnYcf4efF/AVo
UXVj2HD7XjWCzskU0slkGr9sorJKi+OC+kp+pebE9y2RF3F6xNLLIPGO9WLuBWcoqwtq+M2J193
8EJUydyfe6Pf9nHg/93IZVhXWtEvDxe1iY9+qorB3DXniHNyDa/OUe3C+zYmBYx56dbSgSXJE
...
kKpX27a3+0P6ATMpQGWInl2WoZbuHePyp/FUqxyFTXlgV5I/+jMqjde/12HNLjbqW/Qqgfe7Qw9
GjcKgt2OdvtTspJPI2eyuRw0nbr9JKdp6eVP1u3xUyaKN1qYzVksB9vKCe6kqRlV4qfUJP1jvSW
l9OKuSbn5zpK0ouzXl9mNfoARhDv30qIt+8n719Wbh9fb5+Eh++Fj5+K/wWCuWQX"
```

Example PARES Value

PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQUrWYU3NllEUUBAfv0kWl1l91TPXeb
hTowRBpmHkyfPfr5gbiRlFHF6FFzKaDFXoqry4uhTGn77PAvH4SQKp1MvmEbTnYcf4efF/AVoUX
Vj2HD7XjWCzskU0slkGr9sorJKi+OC+kp+pebE9y2RF3F6xNLLIPGO9WLuBWcoqwtq+M2J1938E
JUydyfe6Pf9nHg/93IZVhXWtEvDxe1iY9+qorB3DXniHNyDa/OUe3C+zYmBYx56dbSgSXJE0tT4
EzX+bTT6jSTnxI0+Pw3iwKG4YNkUQ0/mxCNljn1SRsfgupiN8ZG33TzqTsUxwhz0nHhbz4l35U7
ecfHPh9/dnIE6N7aLeZ0ePlTqRp9XtVdfqoUzJ15X88BrmsXGWOZKb6UbLkk3Rp4rGUycg7VXRB
Mbe2OZR0G6ILEVw/N2CuRxUaZ1clhQd553wpwYVCFu4VzM9TQ+4svK6FN3yI/Vt89JXZ9+I4i2b
b+2o69FGRNYYZIgGQIzhFUa/+Pz/VQUysdd8aeOsd6xOKaBl6e9V+P8UKI6KcJPb7p9JMbQBkkU
ofHsFyzqS0CNj18GCjmiJlgm8bHQB8v+yC0/K1tW3pcq8ajhgp8ELeZatIuGjIg+mZr87fM/Pqg
HLo2jqv4rN3+/9VHCd3mWl1+ixXnnMLvLKlxrgXx85qoZEVIv5Vbsbtn/yDkn3lR9teMetAfn3B
kTblP2hSte6ujJXI3GRiaJhCppimMZvc/YnMYsW9ZpOtFhxant685Lbj3r6JrLqDzbZ/KU5PVsz
9vect34eig5I70qyYSZkfR24qSyj6AHLitlDaoqTnXnFFdnaa/LPZlfUBNTe4b2400VlxUSiL4p
SrkOjBfumpbnNOcz6MClW7iFVLbfHgLyauUqut6t2k5IhvNq777SL34WBbXq4eJi1W8gPKTHtKp
Lry7KOfEzx+0IG5V1usPJhJuEIsviNmNZGKcxaGUIYnmlA93XweuvByqM9+dkn4pMS0KATAFwLD
wa/FFhTZHVz6Iu+yMO8UugOU4wUiskqklw0E7+Qagcmql927o6tHkZ1gqqWhY5nIWQyLdLy+z5t
QL2IqBMnoUKa5Bxx93uVC0IAgPuqdw/ak2Q8Z4C4ztfomiIFq6umF8cu43R+x0dZ4D1/WxlQF7L
fXvWSRzw7jTF4Ml33eTbewY6tJoHI6WVkkBVOKXFXFf8pFQOXe0bDf1Iy4CjaE4rgJsdHN9S0BU
pLDPvQ2mZhCJzVWRxpwDy0T+D7wAYi+rgvxStYIw45SU7TsRxOKXq1e552p8ZPqC0jPLlpxXy22
nUBP1VT3ib3YdgYnmzUjCaHuQzKb+eugCFZW/3Zs1qdhPU0hFEmp7rrZbK+UjPK1nL0UHrik3YT
eQROYbMJjsimfDbtc+W9DRRPMoYWyPft8HSpCEQ2IlgCEmYnVlCUKVTT5fKZIsbbjNtZQ4gAIux
zHsczhcRtdIQR43cQOjwAugT3ZO2S1JCblskZ1zs7Nk8lLizKbK0Hfwv6QofB7M2Dq5AkHZhmV2
0zRjtNhS1NHekbc/K3elJmxaOeDzJ4h77MFH0oF0iZ7kqXDlpAhWgPRSSpA/oDjhvOdBlPk3V7n
aZufoEr8mO7cHyHnPHALllPOSdjPPuRef4lyE+Qz7BThEN27rc4qYVrXiP64rvBM7ZLveePUl8F
nJvdxgPudj9Ohf5Hmjf847dv+cdwmnBxo2lBDHAPgUABm0cC9zNR9qMj2N+iusSqhkL6TMLqSn+
yx4k7W7vbMF0fZ01iBwzD/cO85J3bapBtpq5W7Vf8+rmZasmvmj1rihXN35SQze6BSnn0J2cq3l
V+DqPdPwUcA0c3ZNDW/ez1k97U238g3tyR9i2LbaDHlcarzDYNyT2yaDDbf9xTDoe9dQQFwLLu4
ZifvBsFdeJpbtbt8FnSM9mLoaI64djUmer5i80k3oHKwtFtcL7/sVWdYPXTsFIu3r2ksIyGj+Hz
XC/IkSx5UEjyYUilLR2k86agBYq7Ie9k05OuH/kwWGI4SR7i6eI7bEpTFfz9QGvdYbDupKaPbn6
dFetH/rE0pBbTbRqnxSywR/BdZIFh3aI2R7GcQljXoAowPWts8ByBrqOc3758K4FhQcb8U/GzxS
WSMctLaNQaC8rz1YGvrW73Q9PA+tLYz/mwfXG8/Me5+sE+zmkgsPdv2te417sHOe5dR3suu8/7N
WvsWTqF1qF6IeYmYRzEHrXYBrncMqdkZb5otAHOL6D/zx7yJn7fWhrkR6uKW+rTXAtcz/6wx15k
kYGXNGsR295ennIp8t/qO/mphNvXYIDU/ks02OePKC1dH14sO/w6zm0/b34HlHLgVt/MwCSCAjk
FnD32SKhGW7mCouHfbu698AcsnIrA2e1ah0IgciqbcHh3iPf9siUQItw0VfiMD9hq7AKDPBsGPY
IxllgghitpDgGFoI9EE0QZNC/9wOetzioFwIWmj7yb2IUdwDZWo19dqsLXJdNsId/LN9x3/k3+j
0fGt/4YOZjEpCmQT+pMnXjMU/qTNeIESnn5lFen5X86dnGsOpZ2XWT0u1FdnqdRZJQJix/nB4uN
nExiKXvETiZhJ5g+jCqhd3YHTPJ+Nsdpjyikg9hitDjsROIbzCFZczuipvngFKEX8CU4n8UpogY
QnyHKbz5CEnew6FoSsuj7xDj9D6KeBUqcLzFUKdXOL5TMvzMULexioFGvdIwXDFJxSra2CW7JcY
Mj/5hEW+Lktr7PPx1ihjvNsNEYS1LeRirsQH2jKygWcvddZT41lVdXL7+SH6wr/i1fYhs2fZ2ds
232q39KVrbivGrzZ36OH5/aI+K0A73PsACHpcZ4PQWtDpWESgo5TzRivJzJ6zEeEzEmdpNbWly2
U3S8+WMyKk+eVKtK9rEL8fWZ2YixWqbs0M+e3QN1JGHIHqy+cpc8WFL6E29FdcBC1oe182GBUyF
2/zLVhlq/b2MLfzkQMwDBd6gRcjFyIZQG4288fPeuPBSX4e6JTFC3qxG090+yoCL4zK0RR53i5E
AZJ6D4xUQFBAimAJeAcj4se0A02m59rE1mdhqHhI9C0f3dpRBWbLwCNJjaFSjHqL1dUWl6pY02V
O+1qbXddDo6VSEp6kOT//HdRIn4NTvEqXPn9WcJBhRVl7ywFgP8Eq5+2oH8XqFIS3QURuHYhwHU
/y/iHGQVK4o3OAEhgMDBHqAcPwdUu0FTqcspPET4xUm8Sb7t49sDN20k3vIcW1ruXmwaJ8eRjeG
TPsOjwr0yxFu7jve26pkcMjT8AbzJsin8f0c3BT8NdZxvb2NbXqZOHRNBaJ2wSPzv4ZZ2KcXZ7S
shthYj6MT8RgSC+JARxgSN/H7OwXg4vaF34+TmcO/HfqSAvcIkbD/fwV1H+M3xADiWBT+aHkKpX
27a3+0P6ATMpQGWInl2WoZbuHePyp/FUqxyFTXlgV5I/+jMqjde/12HNLjbqW/Qqgfe7Qw9GjcK
gt2OdvtTspJPI2eyuRw0nbr9JKdp6eVP1u3xUyaKN1qYzVksB9vKCe6kqRlV4qfUJP1jvSWl9OK
uSbn5zpK0ouzXl9mNfoARhDv30qIt+8n719Wbh9fb5+Eh++Fj5+K/wWCuWQX

Example Return Values

The result should look like the following:

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6d&AUTHEN
TICATION_STATUS[1]=Y&CAVV[28]=OTJlMzViODhiOTllMjBhYmVkMGU=&ECI[2]=05&XID[28
]=YjM0YTkwNGFkZTI5YmZmZWE1ZmY=
```

NOTE: The = character at the end of the XID value is correct (it is the 28th character).

Step 3 Submit the Payflow Sale or Authorization transaction with buyer authentication data

Direct the sale or authorization transaction (TRXTYPE=S or A) to the test Payflow server: **pilot-payflowpro.paypal.com**.

The response should include a value for CARDSECURE.

To Generate a Particular CARDSECURE value (Visa only)

- Any dollar amount with 11 cents (xx.11) causes CARDSECURE=N
- Any dollar amount with 22 cents (xx.22) causes CARDSECURE=X
- All other amounts cause CARDSECURE=Y

- **If the Cardholder is Enrolled:**

  If the **Validate Authentication** transaction returns a verified enrollment, include the following additional buyer authentication name-value pairs from the **Validate Authentication** response:

  AUTHENTICATION_ID

  AUTHENTICATION_STATUS

  CAVV (The test servers use the following CAVV values for all accounts: ZDQzMTMzMjhhMTc1MzgwZTAwNTA= returns a response of 1, 814UqW4Wg0aBA5w0wR8wuQQFBQA= returns a response of 6, all others return 2.)

  XID (Visa only)

  ECI

- **Otherwise:**

  Include the following additional buyer authentication name-value pairs from the **Verify Enrollment** response:

  AUTHENTICATION_ID

  AUTHENTICATION_STATUS

  ECI

D Deactivating Fraud Protection Services

This appendix describes the process of deactivating Fraud Protection Services.

Deactivating Fraud Protection Services removes the Security menu and Transaction Review functions (making it impossible to settle transactions). Therefore, before deactivating the service, you must first perform the following steps:

1. Turn off filters so that no new transactions are sent to the Fraud review queue.
2. Clear the queue of transactions awaiting review by deciding to accept or reject them.
3. Print hard copies of your audit trails as a permanent record.
4. Once you have completed steps 1 through 3, call Customer Service to request deactivation.

   PayPal deactivates the service. Any remaining transactions settle normally.

D Deactivating Fraud Protection Services

Index

A

Accepted transactions 20
Account Number Velocity Filter 86
Active mode 15
APIs
  documentation 49
  downloading 49
AUTHCODE 66
authentication status 32
AVS Failure Filter 81
AVSADDR 66
AVSZIP 67

B

BIN Risk List Match Filter 86
Buyer Authentication
  examples 37
  logging results 47
  parameters 40
  testing transactions 107
Buyer Authentication Failure Filter 78, 84
Buyer Authentication server 33
Buyer Authentication Service 31
  XMLPay 33

C

Card Security Code Failure Filter 83
CAVV 32
communications errors 73
configuring filters 14
credit card fraud 13

D

deactivation 117
deploying filters 17
documentation
  API 49
downloading APIs 49

E

ECI 32
ECI values 45
E-mail Service Provider Risk List Match Filter 88
enrollment requirements 11

F

Filter Scorecard 22
filter types
  High-risk Address 86
  High-risk Payment 81
  Unusual Order 79
filters
  Account Number Velocity 86
  AVS Failure 81
  BIN Risk List Match 86
  Buyer Authentication Failure 78, 84
  Card Security Code Failure 83
  configuring 14
  defined 13
  E-mail Service Provider Risk List Match 88
  examples 14
  Freight Forwarder Risk List Match 87
  Geo-location Failure 89
  IP Address Match 88
  IP Address Velocity 90
  parameters 52
  Product Watch List 81
  required transaction data 49
  response string 54
  Shipping/Billing Mismatch Filter 80
  testing 95
  Total Item Ceiling 80
  Total Purchase Price Ceiling 79
  USPS Address Validation Failure 87
  ZIP Risk List Match 87
Freight Forwarder Risk List Match Filter 87

G

Geo-location Failure Filter 89

H

hacking 13
High-risk Address Filters 86
High-risk Payment Filters 81

I

instant fulfillment 14
IP Address Match Filter 88
IP Address Velocity Filter 90

L

libraries, .NET 25
libraries, Java 25
logging transaction information 47, 62
logging transaction results 47

M

Merchant Plug-in 32

O

Observe mode 15, 17

P

PAREQ 32
PARES 32
Payflow parameters
  RESULT 73
PNREF 66
  format of value 67
PNREF value 67
Product Watch List Filter 81

R

recurring transactions 14
rejected transactions 20
rejecting transactions 22
RESPMSG 66
RESPMSG value 68
responses 54
  credit card transaction 65
RESULT 66
RESULT value 68
RESULT values
  communication errors 73
Reviewed transactions 20
reviewing transactions 20
risk lists 78

S

Shipping/Billing Mismatch Filter 80

T

Test phase 15
testing 16
  Buyer Authentication transactions 107
  filters 95
Total Item Ceiling Filter 80
Total Purchase Price Ceiling Filter 79
transaction response
  PNREF parameter 67
  RESPMSG parameter 68
  RESULT parameter 68
transaction status values 21
transactions
  logging 62
  rejecting 22

U

Unusual Order Filters 79
USPS Address Validation Failure Filter 87

V

Validate Authentication call 36
VERBOSITY parameter 54
Verify Enrollment call 26, 33

X

XID 32
XMLPay
  Buyer Authentication Service 33

Z

ZIP Risk List Match Filter 87

Index